Jennifer Cobbe

LLB (Hons)

LLM

Big Data, Surveillance, and the Digital Citizen

Thesis submitted for the degree of Doctor of Philosophy

School of Law, Queen's University Belfast

January 2018

Abstract

This thesis provides an analysis of the impact of pervasive online surveillance on the relationship between the digital citizen and corporations, the state, and politics in order to argue that the United Kingdom is emerging as a surveillance state in which individual's relationship with society is remade to their detriment. Original contributions to knowledge are as follows: 1) locating the business model of corporations such as Google and Facebook, identified as surveillance capitalism by Shoshanna Zuboff, in a surveillance studies context and connecting it with Antoinette Rouvroy's algorithmic governmentality so as to discuss its rationality and technology of power; 2) identifying the emergence of a new role for the digital citizen in this business model as a produsumer, characterised by the production of surplus-value generating behavioural data through both production and consumption of digital content; 3) recognising state online surveillance regimes as a digital panopticon involving a new technology of power of algorithmic panoptic uncertainty; 4) assessing the implications of the forthcoming General Data Protection Regulation and the proposed ePrivacy Regulation for voter surveillance and microtargeting practices undertaken by political organisations; and 5) showing how the communications data retention and disclosure framework in Parts 3 and 4 of the Investigatory Powers Act 2016 is incompatible with EU law in light of recent decisions of the CJEU. This thesis does not seek to provide solutions or regulatory recommendations in response to the issues raised, but bring together literature, highlight problems, and propose new concepts in order to establish a basis for further research. In doing so, this thesis adopts a governmentality framework and takes an interdisciplinary approach to address the changing relationship between the citizen and society in the era of big data and online surveillance.

Acknowledgements

I would first of all like to thank the School of Law at Queen's University Belfast for the opportunity to study for a PhD and the Northern Ireland Department for the Economy for their financial support.

I would like to thank as well my supervisors, Professor John Morison and Dr Billy Melo-Araujo, for their invaluable knowledge, comments, and guidance, without which this thesis would never have got anywhere.

I'm grateful to Anthony Behan at IBM for his insightful comments on section of this thesis, as well as Professor Maurice Sunkin at the University of Essex for the opportunity to publish some of this thesis and an anonymous reviewer for their helpful comments on my analysis of the compatibility of Parts 3 and 4 of the Investigatory Powers Act with EU law.

Finally, my thanks go to my parents for everything they have done for me and to the rest of my family and my friends for their unending support over a difficult few years.

Methodology

This thesis consists entirely of library-based research and a review of relevant literature, legislation, case law, and other relevant material up to November 1st 2017.

Contents

Chapter 1 | Introduction

This thesis contends that the United Kingdom is emerging as a surveillance state, characterised by the ubiquitous use of data-producing ICT and the prevalence of internet-enabled surveillance, within which the digital citizen is amenable to various new forms of control based on online surveillance, primarily through social media, search, and other popular internet services but also encompassing data gathering from other sources, which overlap, interact, and together remake the individual's relationship with society to their detriment. The ever-increasing use and importance of the internet within society means that its impact on the relationship between the digital citizen and society is a crucial topic for discussion in the contemporary world. As a result, there is a rich and critical literature on both the interface between technology and society[1] and on surveillance which relies on ICT[2], the internet[3], and big data[4]. But no comprehensive analysis has yet been undertaken which looks at the role in the increasing impact of the internet on society of the particular forms and instances of surveillance-based control discussed in this thesis and which focuses on their interactions and points of overlap and on what they together mean for the digital citizen.

Focusing primarily on the UK (with reference to other countries where relevant) and taking an interdisciplinary approach, drawing on concepts and resources from law, legal theory, political philosophy, surveillance studies, computer science, and from various social sciences, this thesis adopts a governmentality framework to identify, examine, and contextualise for the first time these forms of surveillance-based control to which the individual as a digital citizen in the UK is subject in the contemporary digital world[5].

[1] See, e.g., Morozov, 2013
[2] See, e.g., Bennett et al., 2012
[3] See, e.g., Fuchs et al., 2012
[4] See, e.g., Andrejevic and Gates, 2014
[5] Analyses of internet-enabled surveillance which adopt elements of governmentality have been put forward (see, e.g., Reigeluth, 2014; Klauser and Albrechtslund, 2014; and Birchall, 2016), but none

Governmentality considers power in its constituent parts, involving rationalities (the goals to be achieved through exercises of power), technologies (the strategies and techniques adopted to translate those rationalities into reality), and subjects (those whose behaviour is to be altered in the way desired), and thus facilitates an understanding of why and how power is exercised and of the effect that it has on those over whom it is being exercised[6]. Adopting a governmentality framework therefore permits an analysis of the relationships created and shaped by the power interactions represented by these surveillance-based forms control in which they have an identifiable place and an identifiable function as technologies used to translate rationalities into reality by effecting a change in the behaviour of the digital citizen. In this governmentality-based analysis, the methodological approach taken is that of bringing together and building on the body of existing research so as to identify connections and put forward new theoretical concepts as a basis for future research of both an empirical and theoretical nature.

As such, this thesis introduces new concepts where necessary to account for the phenomena being discussed and makes several original contributions to knowledge. This thesis for the first time connects the surveillance capitalism identified by Shoshanna Zuboff with Antoinette Rouvroy's concept of algorithmic governmentality[7] and proposes the concept of the 'produsumer' to account for the digital citizen's role in this[8]. This thesis also identifies for the first time the governmentality of the digital panopticon as a form of surveillance-based control undertaken by state security and intelligence agencies and involving a new technology of power of algorithmic panoptic uncertainty[9], and establishes the incompatibility with EU law of the UK's communications data retention and disclosure framework under the

has yet sought to adopt a governmentality framework with which to analyse the forms of surveillance discussed here as interrelated and overlapping forms of control so as to provide an account of what they mean for the digital citizen.

[6] See Chapter 2.2 for a fuller discussion of governmentality

[7] See Chapter 3.1.2

[8] See Chapter 3.2.1

[9] See Chapter 4.1.2

Investigatory Powers Act 2016[10]. And this thesis for the first time locates the voter surveillance and microtargeting practices undertaken by political organisations in a governmentality framework and contextualises them alongside surveillance capitalism[11] and, also for the first time, assesses the effect of the forthcoming General Data Protection Regulation and proposed ePrivacy Regulation on these practices[12].

In order to understand and critically discuss new technologies and their impact on society it is important to examine them and their development in the context of society. In the west, this means locating them within the neo-liberalised societies that have developed since the 1970s, each of which have their own particular characteristics but which have all followed a similar general trend (as our focus in this thesis is primarily on the UK, we will discuss neo-liberalism as it has developed the UK with reference to other countries where relevant). In the UK, the neo-liberal ideal of the active, self-managing consumer-citizen when combined with the internet gave birth to the neo-liberalised digital citizen[13], who is amenable to control through various forms of surveillance that would have been impossible in the pre-digital era. These involve new roles for the individual, and allow the digital citizen to be commodified as a data profile to be bought and sold on the advertising market, undermine the sovereignty of the individual that in theory underpins neo-liberalism, erode constitutional norms that may be thought fundamental in a democratic society, and challenge legal frameworks for privacy and data protection. Through a governmentality analysis we will identify the techniques for the exercise of power that underpin this, explain how they operate, and locate them within the new forms of control that come together to form the emerging surveillance state. In doing so, we will determine that, in the UK at least, the internet, while promising to empower the digital citizen, has in fact facilitated a transfer of power away from the digital citizen to corporations, the state, and the political establishment.

[10] See Chapter 6.3
[11] Chapter 5.1.2
[12] See Chapter 6.2
[13] Note that neo-liberal citizenship and neo-liberal *digital* citizenship may have evolved differently in other countries

This chapter will give a broad overview of the argument put forward in this thesis, and will introduce key terms and concepts that we will repeatedly return to. We will first discuss the digital revolution that has transformed society over the last few decades, and the resulting emergence of the digital citizen. We will then see how the data produced by the digital citizen as they go about their lives in the digital world is gathered in big data systems and made sense and use of by algorithms, which play a key role in the forms of control we seek to analyse. Finally, we will identify these as forms of surveillance that facilitate the control of the digital citizen by corporations, the state, and political organisations. In doing so, we will set out the structure of the thesis and will provide a starting point for our analysis.

We begin with the internet revolution.

1.1 | The Internet Revolution

The predecessor of what we now know as the internet was the ARPANET, which started with a single link between computers at UCLA and the Stanford Research Institute in October 1969[14]. The ARPANET was where core technologies of the internet - such as TCP/IP, the communications protocol that underpins all internet traffic – were first implemented and tested. By December 1969 the network had doubled in size to four nodes. Two years later there were 15 nodes, by 1977 there were over 100, and by 1981 there were 213 nodes on the ARPANET[15]. At this time it was still primarily an academic research network, and commercial uses were prohibited (a 1982 MIT guide to the ARPANET, for example, stated that "*Sending electronic mail over the ARPANet for commercial profit or political purposes is both anti-social and illegal*"[16]). The ARPANET would form the core of the internet, which came into being when ARPANET adopted TCP/IP in January 1983 as its sole protocol, replacing the

[14] For a detailed history of the development of the ARPANET and the internet see Leiner et al, 1997
[15] Weber, 2003, p.94
[16] Stacy, 1982

earlier NCP protocol that it had been tested alongside, and enabled connections from other networks so as to form a network of networks[17] (the term 'internet' began as shorthand for 'internetwork', used initially to describe the network of networks). With the adoption of TCP/IP, the ARPANET became a sub-network of the new internet, and since any other network that also used TCP/IP could connect to the internet it opened to use for non-research, commercial purposes. In 1990 the ARPANET was closed, while the internet lived on[18].

Also in 1990, Tim Berners-Lee, a British researcher working at CERN in Switzerland, which had connected to the internet in the late 1980s, released the first version of what he called the World Wide Web[19]. This was a system for connecting text files to each other through links embedded within, making use of HTML ('Hypertext Markup Language') to embed links and format pages (what we now know as webpages, which have since grown beyond containing only text). The first web server was hosted on his office desktop PC, and Berners-Lee released the World Wide Web on a royalty-free basis[20]. With the development of the web, the key features of the internet as we know it today were largely in place. The internet and the World Wide Web are often thought of as being the same thing, but in fact the web is one service of several that run on the internet, with others including email, instant messaging, FTP, and Usenet. In 1993 the first graphical web browser, Mosaic, which later became Netscape, was released, sparking the growth of the web as the primary way by which people use the internet[21].

In 1994 Amazon, then an online bookstore, was founded, growing over the next two decades to become a dominant player in many forms of retail, more valuable than Walmart[22], and the eighth biggest employer in the United States[23]. In 1996 the US Congress passed the Communications Decency Act, section 230

[17] Leiner et al, 1997
[18] Weber, 2003, p.94
[19] World Wide Web Foundation; Connolly, 2000
[20] World Wide Web Foundation
[21] Connolly, 2000
[22] Cheng, 2016
[23] Fortune, *Biggest Employers*

of which established that websites are not responsible for the content that is posted on their pages[24]. This allowed the then nascent Web to flourish, and to this day remains the foundation upon which the ability of websites to publish content posted by users without prior review rests[25]. In 1998 Sergey Brin and Larry Page launched Google, improving on earlier search engines, which often ranked search results alphabetically or chronologically, in that it ranked results by importance based on "*the number and quality of links to a page*"[26], allowing for users to more easily access the sites that they were actually looking for. Early websites were primarily static resources, where information was provided to users without much interaction on their part. As the Web expanded, new developments in HTML and other mark-up languages and technologies such as PhP, CSS, JavaScript, and Ajax allowed websites to be increasingly dynamic, host user-generated content, and facilitate interaction between users. This shift from 'Web 1.0' to 'Web 2.0'[27] facilitated the emergence of social networking sites. Early examples included Friends Reunited, LiveJournal, Myspace, and Bebo, but they were all eventually superseded. FaceMash, which was developed by Mark Zuckerberg in his Harvard dorm room for Harvard students to rate the attractiveness of their peers, became TheFacebook in February 2004 when Zuckerberg switched focus to social networking. Facebook, which dropped the definitive article in 2005, originally only allowed students at Harvard to join, then students at any Ivy League college, then any US college, and then students at any university in selected countries around the world, including the UK[28]. Facebook began to allow the general public to sign up in 2006. It now has over two billion users, located in almost every country on the planet, and is by far the most popular social networking site in the world[29].

A year after Facebook opened to the public, Apple's first iPhone was released. Google followed with the release of the first Android smartphone a year later. While earlier mobile phones had internet capabilities, their small screens and

[24] Communications Decency Act of 1996 s.230
[25] Goldman, 2017
[26] Google, *Facts about Google and Competition*
[27] Cormode and Balachander, 2008
[28] Philips, 2007
[29] Constine, 2017

lack of touch interface greatly limited their usability. With the advent of touchscreens, the internet truly came into people's day-to-day lives. No longer would you need to have access to a computer to use the internet in a meaningful way, it could be carried in your pocket and accessed at your fingertips. Smartphone use grew rapidly, with 52% of British adults owning a smartphone in 2012, increasing to 85% as of 2017[30]. As access to the internet has spread (90% of British households now have an internet connection[31]), so too has the importance of online services in modern life. Online banking, shopping, and social networking are obvious examples, but more generally the internet has taken a central place in modern society.

This digital transformation of society has given birth to the digital citizen. As this thesis seeks to examine the forms of control that people are subject to on the internet, we should establish what we mean when we speak of digital citizens. Various definitions have been proposed, though none are authoritative. For Katz, who coined the term, 'digital citizen' was a general description of the kind of people who used the internet[32]. For Mossberger et al, digital citizens are "*those who use the internet regularly and effectively – that is, on a daily basis*"[33]. Hintz et al describe 'digital citizenship' as "*the (self-)enactment of people's role in society through the use of digital technologies*". For our purposes a digital citizen is, broadly speaking, any individual who in the course of their daily lives partakes in some way in the modern internet-connected world. The digital citizen, for example, uses email, owns a smartphone, has an account with one or more social networking sites, shops online, uses online banking, and so on. While almost all British adults are now digital citizens (80% of British adults now use the internet daily, 73% now access the internet 'on the go' using a mobile phone, 77% have bought something online[34], 97% have used search engines, and 76% use social media[35]), any given digital citizen may be more or less involved in this online world. They may be, say, a young person whose

[30] Deloitte, 2017, p.12
[31] Office for National Statistics, 2017
[32] Katz, 1997
[33] Mossberger et al, 2008, p.1
[34] Office for National Statistics, 2017
[35] Ofcom, 2017, pp.5-6

social life is built around social media and smartphones, or they may be an older person who uses email and Facebook to connect with relatives and friends. The key factor is that they take part in the modern internet-connected world in some way and are therefore susceptible to the forms of control that exist therein. When discussing the digital citizen and digital citizenship in this thesis, then, we are not discussing citizenship in and of itself– we are discussing the ways in which digital citizens (i.e. those who use the internet in the course of their daily lives) interact with the online world.

The digital revolution has taken place at the same time as a revolution in American, British, and other western societies informed by neo-liberal social, economic, and political thought. As a result, and perhaps reflecting the fact that new technologies may be conditioned by the societies in which they grow[36], the role of the digital citizen in relation to the new digital world has developed along largely neo-liberal lines. In this, key aspects of the role of the individual in society envisaged in neo-liberal theory have become embedded in contemporary digital citizenship in these countries. Generally-speaking, although the particular characteristics vary country-to-country, these prioritise an active citizen interacting with a small state, which in digital citizenship in the UK has meant the use of e-government services; they promote the consumer-citizen engaged in perpetual choice-making in pursuit of their own self-interest, which in the UK has produced a digital citizen actively engaged in the marketised arena of individualist forms of online consumer politics; and they mandate individualist self-management and personal responsibility, which in the UK has resulted in a digital citizen tasked with managing both their physical body with digital tools and their digital self through privacy self-management and identity performance.

Crucially, as the digital citizen takes part in the digital world everything they do produces data about them and their lives[37]. This data is not only central to the operation of many online services and powers the digital revolution, but it is

[36] Barber, 2003
[37] For a discussion of what is meant by 'data', see Kitchin, 2014, pp.1- 9

also central to the forms of control to which the digital citizen is subject online. Smartphones, for example, contain within them an array of sensors and apps that feed data back to corporate databases and allow the everyday lives of their owners to be watched, tracked, and analysed. We will now look at how algorithms are harnessed to make sense and use of this data.

1.2 | Big Data and Algorithmic Control

In the digital world almost everything that we do produces data. The volume, variety, and value of this data, as well as the velocity at which it is produced, has led to it being called 'big data'. These 'four v's' are big data's four key characteristics[38]. *Volume* refers to the high volume of data produced by individuals and internet-connected devices and is perhaps the key characteristic of big data; *velocity* refers to the high velocity with which data is produced by individuals and devices; *variety* refers to the high variety in data produced by individuals and devices; and *veracity* refers to the quality of data and the fact that data may be unreliable. A fifth characteristic *value*, referring to the need to collect useful data, is proposed by some. These together give big data a unique character, with very large amounts of information of many different varieties being produced rapidly that can be inputted to algorithms and analysed. And the storage of big data in ever-expanding databases and analysis using increasingly powerful computers and algorithms can give new insights into individuals and their behaviour, giving birth to new business models and new forms of control.

Big data systems do not exist in isolation but operate in concert with other systems, apparatuses, and institutions. They form the central part of 'data assemblages'[39], complex socio-technical systems with multiple entwined

[38] Bent et al, 2017, p.457; see also Kitchin, 2014, pp.67-79, where 7 characteristics of big data are discussed
[39] Kitchin and Lauriault, 2014

components which exist to produce data[40]. These assemblages interact with each other and with a set of contingent and contextual apparatuses and influences which together make and remake assemblages across time and place[41]. As a result, data assemblages are not constructed and do not operate in a neutral, impartial way. They reflect the assumptions, practices, and priorities of those who conceive of, design, and operate them. And as these assumptions, practices, and priorities change and adapt over time, data assemblages exist in a constantly shifting state of being. For illustration, Kitchin and Lauriault give us the example of a census:

> *"the data assemblage of a census consists of a large amalgam of apparatuses and elements that shape how it is formulated, administered, processed, communicated, and how its findings are employed. A census is underpinned by a realist system of thought; it has a diverse set of accompanying forms of supporting documentation; its questions are negotiated by many stakeholders; its costs are a source of contention; its administering and reporting is shaped by legal frameworks and regulations; it is delivered through a diverse set of practices, undertaken by many workers, using a range of materials and infrastructures; and its data feed into all kinds of uses and secondary markets"*[42]

To make sense and use of big data, data assemblages use algorithms. Indeed, such is the fundamental role of algorithms in ICT that Gillespie describes computers as 'algorithm machines'[43]. Algorithms are not a modern invention, or unique to big data, and their use in various forms and for various purposes stretches back millennia. But when put to use in big data they are its true genius, and transform raw data into something useful. Algorithms may be described rather prosaically as "*decision-making parts of code*"[44], but there is

[40] Kitchin and Lauriault, 2014; see also Kitchin, 2014, p.24
[41] Kitchin and Lauriault, 2014
[42] Kitchin and Lauriault, 2014
[43] Gillespie, 2014
[44] Beer, 2017, p.3

more to them than that. While they are indeed increasingly used to make consequential decisions[45], such a description limited only to function overlooks the context in which they exist and the purpose for which decisions are being made. In fact, any given algorithm exists because somebody somewhere has a goal that they wish to attain through algorithmic mediation, whether that's ranking search results or delivering targeted advertising, reflecting the fact that the data assemblages of which they form part are themselves highly contextual and contingent on the priorities and aspirations of those who construct them. An algorithm is a set of pre-determined steps to produce a desired outcome. As Beer says, "*Algorithms are inevitably modelled on visions of the social world, and with outcomes in mind, outcomes influenced by commercial or other interests and agendas*"[46]. Algorithms therefore have a normative power that is lost when they are reduced to a purely functional description. Kitchin points out algorithms are often created to produce outcomes that are not neutral, and that their design and implementation is framed by "*systems of thought and forms of knowledge, modes of political economy, organisational and institutional cultures and politics, governmentalities and legalities, subjectivities and communities*"[47]. As such, a critical discussion of the role of algorithms in contemporary society must consider their context and the purposes for which they are designed and implemented[48].

Hill proposes a definition of 'algorithm' as follows: "*a finite, abstract, effective, compound control structure, imperatively given, accomplishing a given purpose under given provisions*"[49]. Hill says that algorithms are finite in that they allow a representation to be articulated in finite time and space; abstract in that they are general and can be applied beyond a single specific instance of a task; effective in that they are precisely determined and certain to produce the result; provide control in that in terms of code they supply content that brings about some kind of change from one state to another, whether that's a change in a

[45] Diakopoulos, 2013, p.2
[46] Beer, 2017, p.4
[47] Kitchin, 2017, p.18
[48] Kitchin, 2017
[49] Hill, 2016, p.47

variable or a subsequent action; are structured in that they consist of smaller units or steps to be carried out; are imperative in that they give directions or orders; and accomplish a given purpose under given provisions in that they seek to a achieve a certain goal in a certain context[50]. This is a definition that intrinsically recognises both the functional and the normative nature of the algorithm and allows us to discuss algorithms both in terms of what they do and the purpose for which they do it.

And the normative power of algorithms is central to their use in systems for algorithmic control. Lazzarato describes governance as "*the ensemble of techniques and procedures put into place to direct the conduct of men and to take account of the probabilities of their action and their relations*"[51]. Algorithms are tools of governance, enforcing norms, directing conduct, and accounting for the probabilities of users' actions and their relations. We can therefore speak of algorithmic governance, or what some call 'algocracy'[52], as being centred on this kind of exercise of power through both the functional and the normative nature of the algorithm. And Yeung has described 'algorithmic regulation' to mean regulatory governance systems that employ algorithmic decision making[53], involving attempts by any entity to computationally generate knowledge from data in order to regulate behaviour in pursuit of some pre-specified goal. This could be a public transport authority seeking to regulate vehicle movement to optimise traffic flow, a social media company seeking to regulate the behaviour of its users to make it more profitable, or an individual seeking to regulate their own behaviour using a fitness tracker[54]:

> *"I refer to algorithmic regulation as decision-making systems that regulate a domain of activity in order to manage risk or alter behaviour through continual computational generation of knowledge from data emitted and directly collected (in real time on*

[50] Hill, 2016, pp.44-46
[51] Lazzarato, 2009, p.114
[52] See, e.g., Danaher, 2016
[53] Yeung, 2017b
[54] Yeung, 2017b, p.6

> *a continuous basis) from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically refine (or prompt refinement of) the system's operations to attain a pre-specified goal"*[55]

While automated management systems are not new, algorithmic regulation as set out by Yeung describes a more recently-emergent form of control facilitated by predictive analysis of big datasets through machine learning and the automatic use of the insights gained through this analysis in systems for influencing behaviour[56]. Algorithmic regulation systems are qualitatively different from earlier systems in one or both of two ways, each of which involve significant differences in the degree of automation. The first difference results from the ability of machine learning systems to draw inferences and make predictions from big datasets and so generate new information without being specifically programmed to do so[57]. Previous systems, including those which involved sophisticated statistical modelling, generally-speaking lacked these abilities (in particular, earlier statistical modelling systems lacked the ability to 'learn' and react to changing circumstances automatically without being specifically programmed, with models instead being constructed by human statisticians). The second difference between algorithmic regulation systems and previous forms of automated management results from the ability of machine learning systems to automatically use the information which they have generated in influencing behaviour without further human intervention. Previous systems, such as that developed for use by the Fire Department of New York in the 1970s[58], were generally used to inform human decision-making in management, rather than to automatically influence behaviour (and while some earlier systems, such as those used in traffic management, were used to

[55] Yeung, 2017b, p.6
[56] Generally-speaking, where the term 'algorithm' occurs in the remainder of this thesis it is being used in reference to machine learning algorithms.
[57] The ability of machine learning systems to automate the process of building and training a model without specific programming or human intervention is one of their key distinguishing features.
[58] See Flood, 2011

influence behaviour[59], this was less automated and they were not based on machine learning but instead involved statistical modelling).

Algorithmic regulation has the potential to have a significant effect on the world that we inhabit[60]. For example, Beer talks about the 'social power of algorithms'[61], "*the capacity of the algorithm to create, maintain or cement norms and notions of abnormality*"[62]. And Just and Latzer show how algorithms are involved in constructing social reality on social media and other online services[63]. Pointing out that social order is based on a shared social reality, and that "*the realities shaped by automated algorithmic selections codetermine individuals' coordination and cooperation on and beyond the Internet*"[64], they question what impact the increasingly personalised nature of the algorithmic production of social space online has on this shared social reality[65]. They contend that this high degree of personalisation, ultimately based on showing the individual what they want to see, results in different individual realities and amplifies audience fragmentation and individualization[66], leading to isolation of like-minded individuals in echo-chambers where people only have their existing opinions and prejudices confirmed[67]. As these online social spaces are predominantly owned and operated by corporations, and as the ultimate goal of personalising online space in this way is to induce in the user behaviour desired by those corporations, they have a major role in the construction of social reality online which can be directed to suit corporate ends. In a similar way, algorithms have had an impact on many other aspects of contemporary society – as Kitchin notes, with the rise of 'algorithm machines', new forms of algorithmic control are reshaping numerous social and economic systems[68].

[59] See, for example, Light, 2005
[60] See, for example, Kitchin, 2017
[61] Beer, 2017
[62] Beer, 2017, p.7
[63] Just and Latzer, 2017
[64] Just and Latzer, 2017, p.247
[65] Just and Latzer, 2017pp.246-247
[66] Just and Latzer, 2017, p.248
[67] Just and Latzer, 2017, p.249
[68] Kitchin, 2017, pp.14-16

Despite the prominent role of algorithms in the modern world, Diakopoulos points out that we lack clarity about how algorithms exercise their power[69]. As Danaher says, while we may know the inputs and the outputs we often cannot see, or could not understand, the decision-making process of an algorithm itself[70]. Burrell sets out three distinct forms of this 'algorithmic opacity'[71]. The first is intentional opacity, where an algorithm is concealed out of concern for the protection of intellectual property (the precise nature of algorithms is often a closely guarded secret). The second is illiterate opacity, where an algorithm can only be understood by those with the technical ability to read and write code (which remains a specialist skill). And the third is intrinsic opacity, where the ways that an algorithm makes a decision are difficult for humans to understand (known as the 'interoperability problem'[72]). While more than one of these may combine in the same algorithm – it is possible, for example, for an algorithm to be intentionally opaque and for it to be the case that even if it wasn't intentionally opaque then it would still be illiterately or intrinsically opaque - the end result of any one of these forms of opacity is that those subject to the control of the algorithm usually cannot see how it operates, or what goal it is operating in pursuit of. Algorithmic opacity means that, as Pasquale puts it, while authority is increasingly algorithmic, the "*values and prerogatives that the encoded rules enact are hidden within black boxes*"[73]. Thus in algocracy decisions that were once made by humans are made automatically by algorithms in pursuit of human goals but invisible and therefore unknowable to those subject to their control.

The functional and normative nature of algorithms is taken up in many uses. Algorithms, for example, determine the sequencing of traffic lights in intelligent traffic control systems. They are at the heart of the cryptography that underpins modern secure banking, shopping, and communication. It is an algorithm that decides which email is spam and which should go to your inbox. Indeed, the

[69] Diakopoulos, 2013, p.2
[70] Dahaner, 2016
[71] Burrell, 2016; see also Danaher, 2016
[72] Lepri et al, 2007, p.12
[73] Pasquale, 2015, p.8

ways that algorithms are put to use in pursuit of human goals in contemporary society are far too numerous to count. But for our purposes we are interested in how they are used both functionally and normatively in big data systems where the primary source of the data is the life of the digital citizen. In this context, algorithms are crucial components of big data surveillance systems which seek to exert some form of influence over the digital citizen in pursuit of the goals of corporations as they seek profit, of the state as it seeks security, and of political organisations as they seek electoral success. This is what we will move on now to discuss.

1.3 | Surveillance and Power

Data collection has always been about power. The survey that became the Domesday Book was instituted so as to help cement the power of the Norman ruling class and facilitate revenue collection in the decades after the conquest of 1066[74]. In order to govern the kingdom, the King needed to know who was in the kingdom, who owned which parts of the kingdom, and who owed what to the Crown. In 1603, the English cartographer Richard Bartlett was dispatched to Donegal so that he could map its terrain and its people as the English Crown attempted to extend its control over Ireland. The locals, understanding the nature of his endeavour and not wanting their country to be known to the English, removed his head from his body[75]. The Victorians were enthusiastic data collectors[76], measuring and quantifying everything within reach. In the present day, data is collected about us from the moment we are born. Medical staff note the date and time, our birth weight goes into medical records, and our name goes onto a birth certificate and into the register of births. As we grow we are measured and compared to growth charts by which we are held to a standardised norm and deviations from that norm are identified and sought to be corrected. The collection of data about people, their lives, and their

[74] Taylor, 1975
[75] Montano, 2011, p.59; Farrell, 2017, p.31
[76] Goldman, 1991; Mahon, 2009

behaviours are practices by which people are measured, quantified, and recorded for the purposes of government. And we can understand this to be a form of surveillance within the definition put forward by David Lyon:

> *"[surveillance is] any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered"*[77]

Systematic surveillance has long been used for control. Marx wrote in the 1860s of the surveillance of workers in factories by other workers elevated above them in hierarchy for the purpose of watching over them in order to impose the control desired by their employers[78]. Foucault, adopting the metaphor of the panopticon, wrote in the 1970s and 80s of surveillance as being a feature of the disciplinary forms of power in western society[79]. And in the 90s both Deleuze[80] and Gill[81] wrote extensively of surveillance in neo-liberal capitalism arising in the offline world, rather than the online world, but involving the gathering and analysis of data beyond the relatively simple surveillance of employee undertaken by employer (or by another employee acting on their behalf).

Surveillance undertaken with the use of ICT is known as 'dataveillance', a term which was first used by Roger Clarke in 1988 to describe "*the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons*"[82]. Early forms of neo-liberal dataveillance included credit reference services, which use data derived from an individual's past behaviour to attempt to predict the likelihood of them repaying credit and to give an estimated guide to the creditworthiness of the individual and, therefore, the likelihood of a potential creditor profiting from the need to borrow. Gill shows how, particularly in the US, the individual became beholden to credit reference agencies, with 'good' credit becoming an essential

[77] Lyon, 2001, p.2
[78] Marx, 1990, p.450
[79] Foucault, 1991
[80] Deleuze, 1992
[81] Gill, 1995
[82] Clarke, 1988

requirement for full participation in civil society[83]. This is indicative of how dataveillance has long been used to create and maintain a new 'normal' in the neo-liberal project of rule, rendering individuals and society amenable to neo-liberal power structures and forms of government. The presence of dataveillance and dataveillance-based forms of control in modern societies is not a new feature.

What is new in the increasingly digital world is the extent of surveillance that can now be undertaken, the exponentially greater quantity of data from multiple sources that can be fed into algorithms, the powerful algorithmic analysis that can be performed in order to render individuals knowable to a much greater degree, the precision of prediction and control, and the way that these are all brought together in new business models that seek to commodify as much of everyday life as possible in the pursuit of profit, in new ways for the state to pursue security concerns and exclude subversive or extremist ideas, and in new forms of voter surveillance and campaigning by political organisations. These new surveillance-based forms of control interact and overlap, blurring the distinctions between corporate, state, and political power, and together remake the relationship between the digital citizen, the state, and politics to the detriment of the digital citizen.

In 2013 Mayer-Schoenberger and Cukier coined the term 'datafication'[84] for the process of transforming many aspects of everyday life into quantified data for use in ICT systems. According to van Dijck, "*Datafication as a legitimate means to* access*,* understand *and* monitor *people's behavior is becoming a leading principle, not just amongst techno-adepts, but also amongst scholars who see datafication as a revolutionary research opportunity to investigate human conduct*"[85]. Facebook provides an archetypal example of datafication, and Bucher[86] and Helmond and Gerlitz[87] have all shown how by surveilling and

[83] Gill, 1995
[84] Mayer-Schoenberger and Cukier, 2013, p.78
[85] van Dijck, 2014, p.198
[86] Bucher, 2012
[87] Gerlitz and Helmond, 2013

recording the behaviour of its users Facebook has turned social interactions into data to be analysed. This big data describing the behaviour of Facebook's two billion users in great detail can then be put to use by subjecting it to algorithmic analysis so as to identify patterns among and correlations between users, infer unknown information about those users, and predict their future behaviour. This allows that behaviour to be influenced so as to produce profit, by providing carefully targeted links and adverts designed to take the user's attention and persuade them to click, purchase, or follow.

This dataveillance system is made available to advertisers, who purchase access to users so as to make use of these analytical and predictive powers in order to more effectively target them with persuasive advertising. As van Dijck puts it, "*The digital transformation of sociality spawned an industry that builds its prowess on the value of data and metadata*"[88]. In this, the data produced by users as they go about their online lives and describing those lives in great detail – and therefore those users themselves - becomes a commodity to be exploited in the pursuit of profit. This reflects Arvidsson's argument, put forward in 2005, before social media grew into a behemoth, that brands commodify our social lives[89]. This is a process that he described as the "*branding of life*"[90]. The commodification of life takes place not just on Facebook, as similar datafication and commodification can also be seen on many other online platforms.

In recognition of the way that the data produced through this datafication is used, Degli Esposti has updated the definition of dataveillance in order to include attempts to control behaviour. She adds the element of seeking to control behaviour, which reflects Lyon's classic definition of surveillance as involving the collection or processing of personal data for the purpose of influencing or regulating behaviour, to define dataveillance as "*the systematic monitoring of people or groups, by means of digital information management systems, in order to regulate or govern their behaviour*"[91]. This updated and

[88] van Djick, 2014, p.199
[89] Arvidsson, 2005
[90] Arvidsson, 2005, p.251
[91] Degli Esposti, 2014, p.210

extended definition of dataveillance, more in line with the common definition of surveillance and involving the gathering of data about people or groups for use in digital information management systems with the aim of regulating or governing behaviour, can therefore be characterised as surveillance which involves digital information management and data processing systems[92].

Dataveillance in this form is central to surveillance capitalism. This is the business model of the corporations that dominate the digital world, including Google and Facebook. In order to be dataveilled the digital citizen and their behaviour is first datafied. Next, this data is subjected to predictive algorithmic analysis so as to produce new information, both about the individual and about their behaviour. The information produced is then used to predict future behaviour and attempt to direct it in the way desired. Given the centrality of algorithmic analysis to this process, we can recognise dataveillance as a form of the algorithmic regulation described by Yeung.

The unparalleled visibility and knowability of individuals produced by the algorithmic analysis of the big data created by and describing them through the process of datafication and the application of this algorithmically-generated information to powerful predictive models and techniques for influencing behaviour in such a way as to produce a desired action is unique to surveillance capitalism, and distinguishes surveillance undertaken in this way from previous forms of capitalist surveillance. While previously surveillance of employees or customers was used as one technique among many to establish and maintain an order that facilitated the pursuit of profit by other means, surveillance capitalism involves a new order in which pervasive dataveillance as a form of control is itself the defining feature of the order and the primary means by which control is exerted and profit is extracted. In this, the work of the digital citizen in producing behavioural data is exploited, the datafied digital citizen becomes a commodity to be bought and sold on the advertising market, and their agency as a social and economic is appropriated through the highly

[92] This is the definition of 'dataveillance' to be used in this thesis.

personalised, responsive, and persuasive form of behavioural nudging known as hypernudge and directed so as to produce profit for corporation.

The discussion of surveillance capitalism in this thesis will focus primarily on Google and Facebook. While this business model is used by a wide variety of corporations who provide services beyond those provided by these corporations (with Amazon, for example, also employing a variation on the theme), together they represent its progenitor (in the case of Google) and its foremost proponents (in the case of both Google and Facebook). However, the analysis of how surveillance capitalism operates and what it means for the digital citizen would generally-speaking apply equally to the other areas in which this business model is implemented (subject to sector- and implementation-specific modifications, where appropriate).

Dataveillance is also undertaken in the programmes of the state's security and intelligence agencies. The extent of this surveillance, primarily carried out by the National Security Agency ('NSA') in the US and Government Communications Headquarters ('GCHQ') in the UK, was made public by former NSA contractor Edward Snowden in 2013. As well as over 200 interceptors located on the internet backbone cables coming to and from the UK that enable the collection of all the data passing through them as well as the systematic weakening of encryption standards and installation of backdoors in otherwise secure networking equipment, this also involves the provision of data to the security and intelligence agencies from corporations involved in surveillance capitalism. As a result, the practices of surveillance capitalism and the extensive surveillance apparatus developed by these corporations forms a significant part of the state's surveillance operations. As the data held by these corporations relates to almost every aspect of contemporary digital life, the state has access to huge amounts of information about the lives, preferences, and activities of its citizens. As a result, the surveillance operations employed by surveillance capitalism corporations and the state online surveillance regimes operated by GCHQ and the NSA are linked, and represent interrelated forms of control. The data collected by these agencies is funnelled into giant repositories, from where

it can be accessed and algorithmically analysed in order to allow for real-time surveillance of almost any digitally-connected individual in the country and around the world. The potentially all-seeing surveillance system operated by the NSA and GCHQ, the digital panopticon constructed through their extensive surveillance programmes and facilitated by the practices of surveillance capitalism, allows the state to extend its reach into the homes and lives of tens of millions of people.

In the digital panopticon the state no longer needs to involve the populace in their own surveillance through a network of informers, but can rely on the interception of the data that they produce as they go about their online lives and on their access to the data that they willingly give up to surveillance capitalism corporations and which those corporations in turn pass on to the state. And predictive algorithmic analysis of big data allows security and intelligence agencies to infer otherwise unknown information about people, casting algorithms as the new informers in this new form of surveillance. Algorithmic opacity hides these processes in black boxes, invisible and unknowable to those subject to their control. In this, the individual is reduced to a pliant subject of state control, and that control moves to a pre-emptive basis by which everyone is under undue suspicion as a potential criminal, with potential evidence against them gathered, analysed, and stored. And the empirically demonstrated chilling effect of the digital panopticon on freedom of expression potentially excludes subversive ideas and undermines the cornerstone of democracy.

And the growing use of surveillance by political parties and campaigns, often then making use of dataveillance systems constructed by corporations to reach voters directly, is becoming a feature of the political and electoral process in many countries. The ability of political organisations to surveil voters, subject them to similar predictive algorithmic analysis as that performed in surveillance capitalism, and access – at a price – the powerful behavioural modification tools developed by corporations like Facebook and Google brings new influences to politics. The asymmetries of access to data gathering, predictive analytics, and microtargeting tools between wealthy, established political parties and

candidates and those outside the mainstream potentially entrenches the political establishment and dramatically increases the influence of capital on the democratic process. Through this, the agency of the digital citizen as a political actor becomes directed to the pursuit of the goals of political organisations, and the online public sphere is degraded.

These new forms of dataveillance-based control, involving big data and predictive analytics, challenge the existing 'notice and consent' model of privacy and data protection. In a world where it is impossible to know what information about any given individual may be predicted or inferred through the algorithmic analysis of big datasets, and where privacy notices are often long, confusing, and written in obfuscating legalese, it is increasingly difficult for individuals to be given effective notice, let alone give informed consent to the use of their data. The EU's forthcoming General Data Protection Regulation, which seeks to provide a new baseline for data protection, goes some way towards addressing these deficiencies, but as it is itself fundamentally grounded in a notice and consent model it cannot resolve them all. However, privacy and data protection law may provide some recourse for the digital citizen. The voter surveillance and microtargeting operations carried out by political organisations will be subject to restrictions under the GDPR framework, with individuals given new rights over their data and new obligations placed on data controllers. And the existing ePrivacy Directive provides a way for aspects of the digital panopticon, in particular the communications data retention and disclosure provisions of the UK's Investigatory Powers Act 2016, commonly known as the 'snooper's charter', to be challenged in law.

Dataveillance is a form of surveillance which, like all other forms of surveillance, is fundamentally about power and control. Big data takes this to a new level, and the algorithm is central to the exercise of that power in the digital world. This thesis seeks to identify the forms of dataveillance-based power to which the digital citizen is subject online, based on big data, surveillance, and algorithmic and analysis and control, and the ways that they remake the relationship between the digital citizen and the emerging surveillance state. This new

surveillance state represents the instigation of a new relationship between corporations, the state, political organisations, and the digital citizen. Surveillance now reaches deep into our lives in a way that would have been possible in the pre-digital era. In this new relationship, the digital citizen becomes subject to overlapping and complementary forms of surveillance-based control, blurring the lines between corporate, state, and political power. And the digital citizen is remade as an exploited commodity to be bought and sold in surveillance capitalism, a potential criminal in the digital panopticon, and politically manipulable subject of persuasive, microtargeted political advertising. Understanding these new forms of control and their effect on the digital citizen is crucial to understanding the role of the digital citizen in the new digital world.

1.4 | Thesis Overview

This introduction has set out in broad terms the argument put forward in this thesis, which holds that the UK is emerging as a surveillance state, characterised by the ubiquitous use of data-producing ICT and the prevalence of internet-enabled surveillance, within which the neo-liberalised digital citizen is amenable to the identified new forms of surveillance-based control that remake their relationship with corporations, the state, and politics to their detriment. Along the way we have introduced, defined, and contextualised key concepts that will inform our analysis and to which we will repeatedly return as our argument unfolds. The remainder of this thesis proceeds as follows.

In the next chapter, we will discuss the neo-liberalisation of western societies since the late 1970s, in particular the UK, in order to put the development of surveillance-based forms of online control in their social and political context, in which the individual is required to take on a new role as an active, self-managing consumer-citizen engaged in a process of perpetual choice-making in a marketised public and is imbued personal responsibility for their lives regardless of any outside forces that they may encounter. And the emergence of

a neo-liberal form of digital citizenship in this mould will be identified. Governance and governmentality concepts will give us a language with which to discuss power and government in the newly differentiated polity of the neo-liberal state, and to place techniques for the exercise of power through surveillance and the goals and values underpinning them into a theoretical framework in which they have an identifiable place and an identifiable function.

In Chapter 3 we will encounter the business model behind the most successful of the new corporations that dominate the digital world, surveillance capitalism, and will identify this as a new form of capitalism, with a new logic of accumulation and new forms of labour that move beyond existing analyses. We will see how in surveillance capitalism the digital citizen takes on a new role as a source of behavioural data from which great profit is derived, and will see how they become commodified as a data profile to be bought and sold on the advertising market and how their agency as a social and economic actor becomes appropriated and turned against them in pursuit of corporate ends. But we will also see how new forms of everyday resistance have sprung up to resist the practices of surveillance capitalism, and how some of these are beginning to receive tentative recognition in law.

Then, in Chapter 4, we will discuss how the ubiquity of IT in the modern world and the vast quantities of data gathered by surveillance capitalism corporations have been co-opted by the state in order to construct a digital panopticon and exert control over the individual as they move through the online world. We will discuss how mass online surveillance in this way undermines the presumption of innocence, casting the digital citizen as a potential criminal and the data gathered on them by the state as potential evidence. We will also discover how the chilling effect of the digital panopticon on freedom of expression reduces the willingness of the digital citizen to seek out and impart ideas and information that may be considered to be subversive, extreme, or outside the mainstream. In all we will see how the state can now surveil entire populations with an array of devices and minimum active involvement of the populace, reducing them to pliant subjects of the digital panopticon's control.

In Chapter 5, we will examine how voter surveillance by political organisations and the advertising tools provided by surveillance capitalism corporations allow political parties and campaigns to seek to algorithmically engineer online public space. We will see that through this, voters can be microtargeted with personalised, precisely tailored, and highly persuasive political advertising, and that the imbalance of resources between established political organisations and others leads to an imbalance in access to data and to microtargeting tools which entrenches the position of the political establishment and amplifies the influence of capital in the democratic process.

Finally, in Chapter 6, we will address the relationship between these surveillance-based forms of control and privacy and data protection law. In this, we will see how the practices of surveillance capitalism undermine the current 'notice and consent' model, and will discuss the extent to which GDPR has the potential to address these issues. We will also assess whether the voter surveillance and microtargeting discussed in Chapter 5 is compatible with GDPR and with the proposed ePrivacy Regulation, and will set out the rights that voters have to challenge these practices and what obligations will be placed on political organisations as they surveil voters and the surveillance capitalism corporations that facilitate microtargeting. And we will finish by showing that the communications data retention and disclosure regime of the Investigatory Powers Act, commonly known as the snooper's charter, is incompatible with the existing ePrivacy Directive in light of recent decisions of the CJEU.

Now we move on to discuss the transformation in government and society driven by neo-liberal thought, identify the role of the individual within neo-liberal society, introduce our governmentality framework, and establish the neo-liberal nature of contemporary digital citizenship in the UK.

Chapter 2 | Digital Citizenship and the Contemporary State

In the first chapter we described the development of the internet and its impact on society in the last decades of the twentieth century and into the twenty-first, and set out some key concepts in relation to data, surveillance, and algorithmic control. In this chapter we will see that at the same time there has been a revolution in government and society informed by the revival of a modified form of classical liberal economic thinking known as neo-liberalism. This prioritises the role of the free market and of the personally responsible individual actively engaged in civil society, and represents a significant shift away from the previously orthodox model of the welfare state. Barber argues that "*technologies tend not to be determinative but rather are conditioned by what is going on in the society in which they grow*"[1], and it is in the context of increasingly neo-liberal Anglo-American societies that the platforms and services that dominate the internet have emerged. An analysis of how these platforms and services operate and the forms of control to which they subject the individual must take into account the socio-political context in which they exist, namely that of contemporary neo-liberal society.

We will see that as the ever-increasing role of the internet within modern society and the concurrent neo-liberalisation of the state have combined they have created a new form of digital citizenship in this neo-liberal mould. In doing so, we will set some of the foundations for the broader argument put forward in this thesis. This holds that in the emerging surveillance state of the UK the neo-liberalised digital citizen is amenable to new surveillance-based forms of control in pursuit of commercial, security, and political considerations that remake the relationship between the digital citizen and society to the detriment of the digital citizen in terms of their ability to be exploited for profit by private

[1] Barber, 2003

corporations engaged in new forms of surveillance-based capitalism, in terms of how mass online surveillance by the state undermines some of the fundamental norms of democratic society, and terms of the how surveillance and big data techniques allow the online public sphere to be manipulated by political parties and campaigns, contributing to its decline.

This chapter will explore neo-liberalism in theory and identify key themes that provide common ground across its sometimes disparate strands, including the sovereignty and personal responsibility of the individual, the prioritisation of the free market as the guarantor of individual liberty, and the pursuit of a smaller state focused on regulation rather than active economic intervention or provision of public services. We will then look at how neo-liberal policies have been implemented in the UK since the 1970s and what this means for the individual and their role within the state as an active consumer-citizen, which will be identified and described. Next, we will discuss how we can conceive of power, government, and the state. Governance concepts will describe the form of the neo-liberal state as a marketised state, a differentiated network of power relationships between many economic and political actors, and a governmentality framework will locate government as a power interaction between two or more of those actors in the pursuit of some goal and the state as an illusion created by the network of those power interactions. Finally, we will identify contemporary digital citizenship as fitting a neo-liberal mould, interacting with a smaller state facilitated by developments in e-government, operating as an active citizen engaged in consumer forms of politics, and taking individual responsibility for the self in an ongoing process of self-management. As indicated in Chapter 1 and as with the thesis as a whole, our focus is on how neo-liberalism has developed in the UK, although reference is made to other countries where relevant.

In all, neo-liberalism will be placed in a broader theoretical context as an ideology that drives the exercise of power, a rationality of government that has transformed the state and remade the individual within that state as an active self-managing consumer-citizen, and in doing so has set the course for the

emergence of the neo-liberal model of the digital citizen. We will establish how we are to conceptualise *power*, *government*, and the *state* and will contextualise the emergence of this identifiably neo-liberal model of *digital citizenship* in order to provide definitions of and frameworks for these concepts which are central to our analysis.

2.1 | Neo-liberal Concepts of the Citizen and the State

In any discussion of neo-liberalism we must recognise that there are clear differences between neo-liberal theory and neo-liberal practice. Neo-liberalism in theory is a revival of classical liberalism which centres the individual as a sovereign actor and is concerned with providing for the liberty of the individual through the free market. It seeks to reform economies and governments in order to liberalise the economy and allow for the free operation of the market and so guarantee individual liberty. In practice it has generally been implemented by exploiting crises at any opportunity that arises and by framing reform as being in the best interests of the people. In actuality, neo-liberal reform often results in gains for economic elites at expense of others, and in practice doesn't account for imbalances of power and access to information and places responsibility with individuals for failings beyond their control. Ultimately, far from ensuring liberty through the free market, neo-liberalism in practice often leads to a reduction of the economic and political power of the individual.

First we will set out the key points of neo-liberal theory, and we will then see how neo-liberal reform has been implemented in practice since the 1970s, before setting out the principles of neo-liberal citizenship and the role expected of the individual in the neo-liberal state.

2.1.1 | Central Themes of Neo-liberal Theory

While the roots of neo-liberalism stretch back to the 1930s[2], it wasn't until the 1970s that what we now call 'neo-liberalism' got its name. The term 'neo-liberal' as we would understand it today was first given to economic reforms advocated by Milton Friedman and implemented by the Chilean dictator Augusto Pinochet in the early 1970s, which promoted deregulation and free market economics. Neo-liberal thinking is often said to have originated in the 1950s and 1960s in places such as the Mont Pelerin Society and the University of Chicago's Department of Economics – the economists advising Pinochet in Chile were called the 'Chicago Boys' as a result of having studied under Friedman and others in Chicago in the 1950s – as well as in the Austrian School of economic thought, and is in many ways a fusion of the economic thinking of Friedman with Friedrich Hayek's socio-economic philosophy. The commonly held view is that neo-liberalism originated as a concerted effort by right wing economists and activists to counter leftist ideas and promote policies seeking to establish private property rights, free markets, and free trade worldwide, while supporting transnational capitalist interest and blocking attempts to consider alternatives[3]. Here we focus on this post-WW2 neo-liberalism.

Neo-liberalism conceives of the citizen, the state, and the relationship between the two in a way that is fundamentally different from the model that previously dominated in the west. For several decades the post-war consensus in the UK provided for a Keynesian welfare state with a mixed economy, in which the formal state was an active economic actor and controlled key industries, influenced economic development, and provided public services and an extensive social security net for the poor. In this, the individual operated primarily as a recipient of public services and took on a largely passive role as the state took care of many of their needs. At its core, in contrast, neo-liberalism holds that the free market is the only mechanism by which the welfare and liberty of the individual can be guaranteed. According to Bockman:

[2] Brennetot, 2015, pp.30-39
[3] Bockman, 2007

> *"Neo-liberalism is grounded in the assumption that governments cannot create economic growth or provide social welfare; rather, by trying to help, governments make the world worse for everyone, including the poor. Instead, private companies, private individuals, and, most importantly, unhindered markets are best able to generate economic growth and social welfare"*[4]

In pursuit of this, neo-liberalism in theory aims to cut back the formal state so that it provides only the most basic services and guarantees in order to allow the private sector, civil society, and the individual to inhabit the space formerly occupied by the state and to allow the market to operate freely.

While it is difficult to come to a conclusive definition of neo-liberalism[5] or to identify or describe a typical neo-liberal state[6] – and key authorities on neo-liberalism disagree on many aspects – we can identify common themes and fundamental ideas. The 'Washington Consensus' is a term coined in 1989 by economist John Williamson to describe ten key policies endorsed by major economic organisations including the World Bank, the IMF, and the US Treasury Department[7]. These ten policies have over time come to be seen to be a statement of neo-liberal thinking, and the phrase 'Washington Consensus' has come to describe neo-liberal policies generally[8]. These policies include the following: that in fiscal policy governments should avoid running up large deficits; that public spending should be redirected from subsidies; that the tax base should be broadened and tax rates should encourage innovation and efficiency; that interest rates should be market determined; that exchange rates should float; that trade should be liberalised; that investment should be liberalised; that state enterprise should be privatised; that the economy should

[4] Bockman, 2013, p.14
[5] Boas and Gans-Morse, 2009
[6] Harvey, 2005, p.70
[7] Williamson, 1990
[8] Although Williamson contends that the characterisation as a set of neo-liberal policies is incorrect (Williamson, 2002)

be deregulated; and that property rights should be legally secured[9]. Hay identifies eight key themes of neo-liberalism[10], elements of which echo Williamson: the efficiency of the market in allocating resources; the desirability of global free trade and free movement of capital; the desirability of a small, non-interventionist state; the state as a custodian of the free market; individual liberty; elimination of welfare that disincentives participation in the market; labour market flexibility; and the efficiency of the market in providing public goods. We can broadly identify the following key themes of neo-liberal thinking:

1. **Individual Sovereignty.** Neo-liberalism is in theory constructed around the individual, who is characterised as a sovereign[11], autonomous agent interacting with the wider state as active citizen[12] and an emphasis on personal liberty and responsibility. Individual action, active self-government, and promotion of self-interest are therefore central to neo-liberal concepts of the role of the individual within the state[13]. Friedman and Hayek both believed that personal liberty is impossible without economic liberty[14] and neo-liberal theory holds that the individual must take part in the market as an independent sovereign actor exercising their own political, social, and economic agency. As such, there is an emphasis in neo-liberal thought on personal freedom, with individuals as autonomous agents making decisions, pursuing preferences, and seeking to maximise the quality of their lives[15]. This emphasis on personal freedom is built on a Hayekian idea that societies are the aggregate of individuals striving for positive outcomes, or 'utilities', for themselves[16] and aims to open up ways for individuals to attain these 'utilities'. In the UK this idea was famously elucidated by Margaret Thatcher when she was Prime Minister, stating in 1987 that "*there's no such thing [as*

[9] Williamson, 1990
[10] Hay, 2007, p.97
[11] Feller and Spash, 2014
[12] Powell and Steel, 2012, p.2
[13] Harvey, 2005, p.68
[14] Hayek, 2001
[15] Rose and Miller, 1992, p.34
[16] Corbett and Walker, 2012, p.489

society]! There are individual men and women and there are families. And no government can do anything except through people, and people must look after themselves first"[17].

2. **Prioritising the free market**. As neo-liberalism puts forward a belief in the free market as the ultimate guarantor of individual liberty[18], it calls for the prioritisation of the free market above virtually all else. Hayek writing in 1978 argued that "*If Mrs. Thatcher said that free choice is to be exercised more in the market place than in the ballot box, she has merely uttered the truism that the first is indispensable for individual freedom, while the second is not: free choice can at least exist under a dictatorship that can limit itself but not under the government of an unlimited democracy which cannot*"[19]. In Hayek's view, personal freedom is impossible without economic liberty[20]. Friedman likewise wrote that "*Historical evidence speaks with a single voice on the relation between political freedom and a free market. I know of no example in time or place of a society that has been marked by a large measure of political freedom, and that has not also used something comparable to a free market to organize the bulk of economic activity*"[21]. Neo-liberal policies – in contrast to the Keynesian view, which promotes state intervention in the economy – prioritise laissez-faire economics and the restriction of welfare systems, which are characterised as providing a disincentive to the individual from operating fully in the market and, therefore, a barrier to personal liberty. However, Hayek did advocate for the provision of some basic social welfare in order to prevent absolute poverty and where necessary provide for the minimum of food, shelter, and clothing needed to preserve health, and argued that the state should provide a comprehensive system of social insurance to assist in dealing with sickness and accidental injury[22]. This acceptance of the need for some

[17] Keay, 1987, pp. 28-30
[18] Hayek, 2001; Friedman, 1962
[19] Hayek, 1978
[20] Hayek, 2001
[21] Friedman, 1962, p.9
[22] Hayek, 2001, p.148

degree of government-provided social welfare is one of the features distinguishing neo-liberalism from classical liberalism.

3. **A small state with limited power**. Neo-liberalism emphasises a reduction of the formal state to only that required to provide the most basic of public services (including, for example, the protection of private property, the maintenance of order, and some protection for the poor[23]). Neo-liberalism does not seek to abolish the state completely – it seeks instead to create a new form of state that promotes the free market and the power of capital. A central aspect of this is the idea that the formal state should retreat to leave as much as possible to the free market while maintaining a basic regulatory role. It is generally accepted in neo-liberal thought that the state should, for example, ensure legal equality and the rule of law, guarantee property rights, and protect contracts, which are all seen as prerequisites for the proper functioning of the market. Hayek argued that it may be necessary for the proper operation of the market that the state should set basic rules for production such as regulations for the safety of the worker[24], and he accepted that there was a role for government in environmental protection and in preventing fraud[25]. As Carty argues, far from abolishing the state the end goal of neo-liberalism is to turn the nation-state into the market-state[26].

Neo-liberalism, then, can be distilled into these three central principles; the first and most of important of which being an emphasis on the personal responsibility and agency of the individual acting as a sovereign actor within the free market. Continual reform is a hallmark of the neo-liberal state, with reorganisation and institutional re-arrangement a central aspect of its attempts to neo-liberalise and maintain competitiveness in relation to other states operating in the global market[27]. This drive to reform has led to the gradual

[23] Bockman, 2013, p.14
[24] Hayek, 2001, p.43
[25] Hayek, 2001, p.45
[26] Carty, 2008, p.170
[27] Harvey, 2005, p.64

eradication of older, non neo-liberal governing structures and practices and the development of the neo-liberal state.

2.1.2 | The Entrenchment of Neo-liberalism

While we can identify the central themes of neo-liberal thinking, we must also look at how neo-liberal reform operates in practice. In a process beginning in the late 1970s, the post-war consensus in the UK was overturned, bringing an end to the welfare state model of government, and neo-liberal policies and practices became the generally accepted norm in western society. This has been seen by some Marxist academics as a capitalist response to the economic crises that plagued the global economy in the 1970s[28]. With stagflation, a sharp rise in oil prices, debt crises, and fiscal crises, capitalism worldwide was under pressure, reducing profits and control over the economy at a time when socialist ideas enjoyed widespread popularity[29]. These crises led to the decline of the post-war consensus and ultimately the elections of Margaret Thatcher in the UK in 1979 and Ronald Reagan in the US in 1981. Both leaders set about deconstructing the formal state and implementing neo-liberal policies and practices, exploiting opportunities to re-engineer the state. As Burris argues, since then "*[neo-liberalism's] program for 'rightizing' government, and promoting efficiency and effectiveness through harnessing the power of the market within government and across society, has made huge inroads into reforming all manner of social services, ranging from health to housing to human security*"[30].

We should note that while many policies implemented both in the UK and elsewhere since the 1970s can be broadly located within a neo-liberal reforming narrative, and while it is certainly the case that the general trend has been towards reform along neo-liberal lines, the reforming zeal has not always taken a direction that follows neo-liberal theory and has, at times, seemed at odds with its central tenets. As Harvey notes, it's relatively straightforward to define the role of the state in neo-liberal theory, but in practice the process of neo-

[28] Bockman, 2013, p.14
[29] Bockman, 2013, p.14
[30] Burris et al, 2008, p.47

liberalisation has at times evolved away from the template provided by that theory[31]. Practice has often been opportunistic in nature rather than ideologically driven. We should therefore be careful to not assume that all reform is strictly neo-liberal in nature – governments at times implement policies that seemingly contravene neo-liberal thinking. But we can identify the general trend of neo-liberalization and the policies and practices that have contributed to this trend: framing reform as being in the best interests of the pubic and so prioritising the performance of the economy and the free market as the ultimate indicator of good government and guarantor of national welfare, and taking advantage of any opportunities that arise to pursue reform.

Framing Reform

Chomsky identifies neo-liberalism as the latest in a line of 'bad ideas' for economic development that not only fail to serve their expressed goals, but typically turn out to be very good ideas for those promoting them[32]. Citing previous 'bad ideas' from the Permanent Settlement imposed on India by the British Empire[33] through to American economic experimentation in Brazil and Mexico in the post-WW2 period[34], Chomsky argues that throughout modern history economic policies that have enriched the already wealthy and impoverished the already poor have been hailed as economic miracles while concealing their true cost[35]. In practice, neo-liberal reforms transformed Chile into South America's strongest economy, with a decidedly pro-business climate, but were accompanied by authoritarianism and caused significant increases in unemployment and inequality. And, in the UK, Thatcher is often seen as leading a reforming government which brought a level of wealth and prosperity to some that has been described as an economic miracle[36]. Yet her policies also led to levels of unemployment unseen since the 1930s[37], had serious negative effects

[31] Harvey, 2005, p.64
[32] Chomsky, 1999, p.26
[33] Chomsky, 1999, p.26
[34] Chomsky, 1999, p.27
[35] Chomsky, 1999, pp.26-27
[36] Layard and Nickell, 1989; Healey, 2002
[37] Denman and McDonald, 1996

on the working class and arguably helped undermine the cohesiveness of British society as a whole[38], and, alongside similar reforms in the US, set the foundations of economic deregulation that ultimately contributed to the global financial crisis two decades later[39]. And O'Mahony et al identify neo-liberalism as being responsible for the emergence of a 'precariat' in Britain characterised by acute socio-economic insecurity[40]. Even the IMF, long a champion of neo-liberalism, has concluded of some neo-liberal policies implemented in the west that there are prominent costs in terms of increased inequality[41]. Whether we accept Chomsky's characterisation of neo-liberalism as a 'bad idea' or conclude that it is in implementation where inequality arises, neo-liberalism in practice serves to enrich the wealthy at the expense of the poor.

Despite this, in order for the proponents of neo-liberalism to succeed they must convince the people that reform is in the interest of society as a whole. Krugman says that bad ideas flourish because they are in the interest of the powerful[42]. But this is not itself enough. Gramsci argued that in order for capitalism to succeed its supporters must convince the rest of society that the interests of capitalism are the interests of society; that people must be convinced that the aims of those in charge align with the interests of the population as a whole[43]. And this can be seen in the neo-liberal reforming project – according to Chomsky, "*At their most eloquent, proponents of neoliberalism sound as if they are doing poor people, the environment, and everybody else a tremendous service as they enact policies on behalf of the wealthy few*"[44]. To this end, the free market and the performance of the national economy, rather than any other indicator of the well-being of the nation as a whole, has over time come to be framed as the ultimate measure of a government's performance and the primary way by which leaders can demonstrate that they are governing in the best interests of the people.

[38] Wilkinson and Pickett, 2013
[39] Kotz, 2009
[40] O'Mahony et al, 2015, p.25
[41] Ostry et al, 2016
[42] Chomsky, 1999, p.25
[43] Kearney, 1994, p.183 – quoting Gramsci
[44] Chomsky, 1989, p.8

Stephen Gill's 'new constitutionalism' is primarily concerned with describing this. He shows how neo-liberal reforms seek to 'lock in'[45] the power gains of capital, resulting in what he terms 'disciplinary neo-liberalism'[46]. He characterises a new constitutionalist state as being one in which power is decentralised, or, as he puts it, "*the subordination of the state to civil society*"[47]. Gill argues that neo-liberalism has promoted the structural power of capital and subjected the state to market discipline to the extent that governments now seek to prove their credibility and the consistency of their policies according to the confidence that they inspire in financial markets[48]. This primacy of capital has been established over several decades and marks a fundamental reorganisation of the state and its relationship with the public. Whereas previously the priority of the state was directly providing for the welfare of its citizens, the priority of the state in a neo-liberal context is the free market and the power of capital. This ultimately reflects the Hayekian idea that the security, liberty, and welfare of the individual can only be guaranteed by a market free from governmental interference, with neo-liberal reform and the prioritisation of capital and the free market routinely framed as being in the best interests of the people.

Pursuing Reform

Osborne and Gaebler described a process of 'Reinventing Government'[49], driven by neo-liberal ideas of a smaller state and involving shrinking the state by divesting it of the direct provision of various public services and the re-configuring of related power structures. Out of this came the idea of 'modernised' government, expressed in similar terms to those identified in the concepts of New Public Management identified by Hood[50]. These characterise modernised government as broadly seeking out a 'marketisation' of civil

[45] Gill, 2000, p.6
[46] Gill, 2000
[47] Gill, 2000, p.6; this reflects in some ways Kotz's argument that neo-liberalism is the domination of labour by capital (Kotz, 2015, p.43)
[48] Gill, 2000
[49] Osborne and Gaebler, 1992
[50] Hood, 1991

society[51], reflecting Carty's observation that neo-liberalism involves a shift from the nation state to the market state[52]. Hood sets out four administrative 'megatrends'[53] characteristic of New Public Management that we can recognise as aspects of modernised government and neo-liberal concepts of the state: 1) attempts to reverse government growth by reducing staff and expenditure, 2) a shift towards privatization of public services, 3) the development of automation, particularly in relation to ICT, and 4) the development of a more international agenda.

Klein argues that neo-liberal policies have been implemented through the deliberate application of a number of 'shocks' to economies in crisis[54]. According to Klein, crises are used as justification for implementing a range of economically liberalising (or, she says, exploitative[55]) reforms. In Klein's view, economic crises are cynically exploited in order to implement neo-liberal policies. This idea was first described by Friedman in a 1975 letter to Pinochet, in which he advocating neo-liberal economic reform that he described as 'shock treatment'[56]. In Friedman's formulation, endorsed and promoted by Jeffrey Sachs[57], this referred to the sudden introduction of neo-liberal policies, including trade liberalisation, privatisation, elimination of currency controls, and withdrawal of subsidies, with the intention of stabilising the economy and stimulating growth. And in much the same way as neo-liberal policies were adopted in response to challenges facing capitalism in the 1970s, subsequent crises have led to the adoption of increasingly neo-liberal policies and governing practices. This process of opportunistically introducing and entrenching neo-liberalism through a series of shocks in response to crisis can also be seen in the countries of the former Eastern bloc after the fall of the USSR, where Sachs helped guide economic reform[58].

[51] Giritli Nygren, 2009, p.61
[52] Carty, 2008, p.170
[53] Hood, 1991, p.3
[54] Klein, 2007
[55] Klein, 2007
[56] Friedman and Friedman, 1998, p.592
[57] Passell, 1993
[58] Passell, 1993; Sachs, 2012; Harvey, 2005, p.71

In the UK, vast swathes of the public have been privatised since 1979. While by the late 1970s nationalised industries accounted for around 10% of the UK's GDP[59], through the 1980s and into the 1990s over 50 companies – spanning sectors central to the economic life of the country such as energy generation and supply, telecommunications, railways, water supply, steel production, coal production, car manufacturing, aerospace, airports, and shipbuilding – passed from public into private ownership[60]. Privatisation has continued into the twenty-first century, with probation services, air traffic control, English local bus services, and Royal Mail, among many others, either being privatised or part-privatised. Many still nominally public services have been contracted out to the private sector, and private finance initiatives have brought significant private ownership of public infrastructure. This has often been accompanied by efforts to actively involve the people in the privatisation of their own services by offering them the chance to purchase shares in the new corporations at their own expense in order to retain an interest in what was previously in public ownership, and often had been for decades. Bockman describes how privatisation has meant that, rather than having to generate profit from their own enterprise, the private sector has been able to profit from entities that had been created and built by the public[61].

Where industries and public services were privatised, the government shifted its role away from controlling aspects of the economy and directly providing services to overseeing the actions of private agents. This meant the replacement of the welfare state with one that has been characterised as a 'regulatory state'[62], concerned with 'steering rather than rowing'[63]. This regulatory role – often carried out with a light touch and in the pursuit of ever-weaker regulation of the market – removed the formal state from direct involvement in many areas of the economy and left much of what had previously been the accepted role of

[59] Osborne, 2013
[60] Osborne, 2013
[61] Bockman, 2014, p.14
[62] Majone, 1997; Glaesar and Shliefer, 2003
[63] Osborne and Gaebler, 1992

government largely to the private sector. What regulation remains is often weak and ineffective and has rarely been successful, as Burris notes:

> *"the impact of such systems for regulation has often been poor … the most powerful corporate actors have been able to hijack weak systems of accountability in service of their own ends. Some speak of the diffusion of a global system of regulatory capitalism in which governance is operated in the interest of a corporatocracy that populates power positions in government and industry"*[64].

This transfer of economic power and public services from the control of the democratic institutions of government to the private sector underlies the fundamentally anti-democratic nature of neo-liberalism. Cloaked in the language of improved services, better economic outcomes, and more choice for the individual, this shift has resulted in many aspects of what were previously considered the central role of the government moving beyond democratic control. Citizens are no longer to exercise the power of democracy to make their voices heard, but are now consumers who are to make choices as one agent among many within the free market. Ultimately, as a result of neo-liberal reform, it is that market and economic actors within rather than the democratically elected government that now holds power over many areas.

2.1.3 | Neo-liberal Government and the Individual

As we have seen, in the late twentieth century the previously accepted model of western society underwent a revolution informed by neo-liberal ideas of thinkers such as Hayek and Friedman[65]. We will now see how neo-liberalism requires that the citizen takes a much greater role in the management of their lives and in their own self-government within the neo-liberal state[66]. The welfare state expected the individual to be a citizen-subject[67], acting primarily

[64] Burris, 2008, p.36
[65] Hood, 1991; Osborne and Gaebler, 1992; Rhodes, 1997; Rose, 1999
[66] Miller and Rose, 1990
[67] Hewitt, 2001, p.258

as a recipient of government services (e.g. individuals visiting the local GP assigned to them, with services being provided directly by the state). But the marketised state of neo-liberalism requires them to be actively engaged citizen-consumers[68], taking on personal responsibility for their lives as sovereign actors[69]. This required a remaking of the citizen-state relationship on neo-liberal foundations, in which citizens are actively engaging with government and civil society and making choices to interact with public services that, while still funded by the state[70], may be provided by entities lying far beyond the state itself (e.g. individuals actively choosing which privately-operated but publicly-funded GP to visit when they are ill). In theory, this allows the individual significant personal liberty, making choices for their own benefit and pursuing their individual wants and needs rather than the wants and needs of society in general.

Powell and Steel argue that central to neo-liberal forms of modernised government is the self-managing consumer-citizen engaged in perpetual choice-making[71]:

> *"Neo-liberal governance emphasises enterprise as an individual and corporate strategy, supported by its concomitant discourse of marketisation and the role of consumers. The strategy increasingly relies on individuals to make their own arrangements with respect to welfare and support, accompanied by the rhetoric of choice, self-management, responsibility and obligation*[72]

In this model, citizens are required to be actively engaged with civil society[73], making choices from an array of options that may more closely resemble a consumer in a retail environment choosing between a range of similar products

[68] Powell and Steel, 2012, p.2
[69] Beck and Beck-Gernsheim, 2001
[70] Clarke, 2004
[71] Powell and Steel, 2012, p.2
[72] Powell and Steel, 2012, p.2
[73] Miller and Rose, 1990

with differing features and specifications than the recipient of generic services provided the state. Giritli Nygren notes that Foucault, reflecting this, describes the development of neo-liberal government as a transition in the modern state from a civil society to a social market[74]. And, according to Powell and Steel, "*neo-liberalism is especially concerned with inculcating a new set of values and objectives orientated towards incorporating citizens as both players and partners in a marketized system*"[75]. This form of active consumer-citizenship derives from the emphasis placed on a market free from government interference and the sovereignty and personal responsibility of the self-managing individual[76]. In some implementations of modernised services, such as the personalised health budgets that have been introduced in the NHS in England[77], individuals are essentially to determine their own requirements so as to 'pick and choose' from a range of options to put together a personalised set of services – some of which are provided by the public sector, some by the private – that meet their needs but remain centrally funded by the state.

Those encouraging citizen choice-making in this marketised arena often point to improved outcomes for service users and a reduction in the resources required to be provided by the state (indeed, large-scale trials of personal health budgets in England found that they led to generally positive experiences for patients and reduced costs for the NHS, while reducing the number of hospital stays and thus further freeing resources[78]). But equally it assumes – not always fairly or correctly – a capacity in each individual to self-manage to the extent required to be an active, engaged, and, above all, effective choice-making citizen. The marketised neo-liberal state places, for example, an onus on the individual to inform themselves about their options in order to be able to act in their best interest at all times. Being capable of self-informing renders the individual capable of effectively self-governing in a neo-liberal way. Ideally individuals are

[74] Giritli Nygren, 2009, p.61, citing Burchell, 1992 and Barry et al, 1996
[75] Powell and Steel, 2012, p.4; see also Carty, 2008, p.170
[76] Beck and Beck-Gernsheim, 2001
[77] NHS Choices – Personal Health Budgets [http://www.nhs.uk/choiceintheNHS/Yourchoices/personal-health-budgets/Pages/about-personal-health-budgets.aspx]
[78] Porter and Simpson, 2013, pp.18-20

capable of self-informing to the extent that, once the relevant information has been made available in some way, they can be left to avail themselves of it make their choices without the need for further direct intervention by the state other than providing funding.

But emphasising personal responsibility also requires the citizen to actively self-manage in other ways in order to maintain their selves, maintain their relationships with other actors, and put themselves in the best possible position from which to exercise their agency. This means, for example, requiring active management of the self not just in terms of information gathering but also in terms of managing their health, their personal finances, and their privacy. This has been noted to be a recurring problem with neo-liberalism that ultimately leaves the individual responsible for failings that may be beyond their control[79]. In practice, all individuals are often assumed to have the same access to information and the same ability to exercise agency and thus there are presumed to be no imbalances of power[80]. As such, and regardless of any evidence to the contrary, the perceived success or failure of the individual in neo-liberalism is not attributed to any systemic, structural, or societal factor that may have disadvantaged, hindered, or benefited them, but is invariably attributed near-exclusively to the individual's personal failings or lack of entrepreneurial spirit. It is seen as the fault solely of the individual if they suffer any detriment as a result of their inability to properly fulfil the role mandated to them by neo-liberalism[81].

This, then, is the role of the individual in the neo-liberal state: that of the active, self-managing consumer-citizen perpetually engaged in a process of choice-making as they exercise their social, economic, and political agency as a sovereign actor striving for the best outcome for themselves in the marketised state and ultimately personally responsible for any failings.

[79] Harvey, 2005, p.68
[80] Harvey, 2005, p.68
[81] Beck and Beck-Gernsheim, 2001; Bauman, 2007; pp.58-59; Bockman, 2013, p.15

2.2 | Conceptualising the State

So far we have set out key points of neo-liberal theory and discussed the process of neo-liberalisation and how this has transformed both the state and the role of the individual. The changes that resulted from this shift in ideological foundation and the subsequent restructuring of the state involve a shift in government from a monolithic entity to a multi-stakeholder dispersed polity. This move towards a more dispersed system, described variously as "*unstructured complexity*"[82] and as "*a differentiated polity*"[83], has been characterised as a move from 'government' to 'governance'[84]. Multi-level governance theories focus on dispersed power, and a network of actors and sites of power interacting to form a whole. We will discuss governance concepts of power and government before building on these with a governmentality framework that gives us the tools to describe and analyse the forms of control to which the active consumer-citizen is subject in the differentiated polity of the neo-liberal state.

2.2.1 | Power and Government

Rose describes the descriptive theme of governance as being concerned with outcomes of the interactions of a range of actors[85]. Rather than being concerned solely with direct interactions between the citizen and the state in which the state is the provider and the citizen the recipient of services, governance theories reflect the shift in governmental ideology and structure over the last few decades and consequently seek to view a wider range of interactions between citizens, the state, and private entities, as well as the relationships between these actors that underpin those interactions. Rose argues that as we move towards a more identifiably neo-liberal structure, "*a new set of political rationalities, [and] governmental technologies…begin to take shape*"[86]. The

[82] Jessop, 2004
[83] Rhodes, 1997
[84] Stubbs, 2005, p.67; Kennett, 2010, p.20
[85] Rose, 1999, p.17
[86] Rose, 1999, p.136

underlying thought processes behind the shift towards modernised government and a marketised state are fundamentally different from those that informed the welfare state model of the citizen-subject. As the structure of the public changes, so rationalities and techniques are identified and adopted to justify, explain, and enable these transformations. Governance theories seek to explain these changes and describe a multi-level polity involving a range of actors in government and civil society as well as citizens all autonomously exercising agency within that polity.

Central to understanding how different actors exercise agency within this multi-level polity is identifying what power is and how it functions in society. Weber wrote that power could be identified as "*the probability that a command with a given specific content will be obeyed by a group of persons*"[87]. For Dyrberg, power consists of the "*power to*" and the "*power over*"[88]. Savoie likewise says that power is made up of two parts: "*someone or some body to give a command and someone or some body with an obligation, a duty, or a desire to obey*"[89]. Morriss argues that "*power is neither a* thing *(a resource or vehicle) nor an* event *(an exercise of power): it is a capacity*"[90]. Foucault, for his part, held that power "*must be understood in the first instance as the multiplicity of force relations immanent in the sphere in which they operate and that constitute their own organization*"[91]. We might consider all of these, and determine that power is the capacity to perform a certain act or to bring about a change in behaviour, or the performance of certain behaviour, in another. We should therefore look at the exercise of power as an interaction between two or more actors with one having the capacity to bring about a change in behaviour, or the performance of a certain behaviour, by the other actors through that interaction. In terms of how power functions in neo-liberal societies, Rose says that "*power is not so much a matter of imposing constraints upon citizens as of 'making up' citizens capable of bearing a kind of regulated freedom…most individuals are not merely the subjects*

[87] Weber, 1978, p.55
[88] Dyrberg, 1997, p.135
[89] Savoie, 2010, p.4
[90] Morriss, 1987, p.19
[91] Morriss, 1987, p.37, quoting Foucault, 2004b

of power but play a part in its operations"[92]. Individuals are not merely subservient to the rule of the state but are actively involved in the continual cycling of power through the system. In the neo-liberal state, individuals are social, political, and economic actors – not just in any public role or office but in exercising their own agency – and they operate within power structures alongside and in interaction with others. This multi-dimensional system of power relations, with individuals autonomously exercising agency in a system where power can be held by any actor who may exercise that power to influence the behaviour of any other, contrasts sharply with the concept of the citizen of the welfare state, where the individual acted largely as a "*thrifty, industrious, and socially responsible*"[93] citizen in adherence to the rules set by the state in return for the government taking care of their needs.

The decisions made by and actions of these autonomous agents are ultimately a product of external influences, beliefs held, outcomes desired, and rationalisations undertaken. If we are to properly understand the interactions between such agents – whether they are individuals, policy makers in government, or those running private corporations – we must seek to understand as far as possible their motivations[94]. To this end, Foucault identified the existence of what he called 'rationalities'[95]. These are ways of "*ways of rendering reality thinkable in such a way that it was amenable to calculation and programming*"[96] – of thinking about, or *rationalising*, power structures, their extent, and the exercise of power[97]. They necessarily reflect the conceptions held by these actors and their determination of their place in the system and that of others:

> *"One isn't assessing things in terms of an absolute against which they could be evaluated as constituting more or less perfect forms of*

[92] Rose and Miller, 1992, p.3
[93] Rose and Miller, 1992, p.24
[94] Bevir and Rodes, 2003, p. 18
[95] Miller and Rose, 2008, p.19
[96] Miller and Rose, 2008, p.15
[97] Rose, 1999, p.26

> *rationality, but rather examining how forms of rationality inscribe themselves in practices or systems of practices, and what role they play within them, because it's true that 'practices' don't exist without a certain regime of rationality"*[98]

And if we want to understand power interactions then once we have identified the rationalities at play within power structures we must attempt to identify how the actors within those structures seek to exercise their power. Foucault theorised that in exercising power there are two kinds of 'technique'. The first are the technologies of the self[99] – the ways that actors come to control their own behaviour based on a range of beliefs and desires in an attempt to attain the 'utilities' identified by Hayek. The second are the technologies of coercion[100], or the ways that actors seek to influence the behaviour of others in order to bring about in them behaviour that the influencing actor has determined to be desirable (the techniques and strategies "*imbued with aspirations for the shaping of conduct in the hope of producing certain desired effects and averting certain undesired events*"[101]). The 'contact point' between these two technologies of power, where the desires and actions of one actor are driven by the power of another, Foucault called "*government*"[102]. Government involves, as Foucault argued, the "*conduct of conduct*"[103].

As Dean notes, in this analysis government "*involves some sort of attempt to deliberate on and to direct human conduct*"[104]. It therefore requires deliberation (which we can see as rationalising the actual or potential behaviour and position of the actors within the power structure – coming to a particular *rationality*) and direction (which we can see as the techniques used to affect the behaviour of another actor within the power structure in order to align it with the decided upon rationality – the employment of a particular *technology of*

[98] Lemke, 2000, p.7 quoting Foucault, 1991, p.79
[99] Foucault, 1993, p.203
[100] Foucault, 1993, p.203
[101] Rose, 1999, p.52
[102] Foucault, 1993, p.203
[103] Lemke, 2001, p.191
[104] Dean, 1999, p.19

power). Inherent in this idea of deliberating on and directing conduct is a power relationship in which government is a type of power interaction – one actor conducting the conduct of another. Savoie observes that power is to politics as energy is to physics – it is the fundamental concept and it takes many forms[105]. We may extend this to say that power is to *government* as energy is to physics. The contact point where government occurs is an interaction between one actor and another. In this interaction power is the fundamental concept, and just like energy it takes many forms. Indeed, Jessop characterised government as "*strategic codification of power relations*"[106], reflecting this link between government and power. We can now say what government consists of (a power interaction) and where it is located (at a contact point between the technologies of power of two or more actors). In understanding how power is exercised we are thus primarily concerned with understanding government. If we are to contextualise and understand the forms of power to which the individual is subject in the digital world then we must understand government, and to do that we must look to these interactions where the power of one actor meets that of another – at the 'contact point' of government-type power interactions – and to the rationalities that underpin them.

2.2.2 | Governmentality and the State

Government, as we have seen, is at its core a power relationship, and can involve any combination of actors. Where governance theories are concerned with what 'what' and the 'why' of modern government, governmentality theories, originating with Foucault in the late 1970s, provide a framework which seeks to explain the 'why' and the 'how'. The term 'governmentality' is used somewhat inconsistently by Foucault[107], but it is not concerned with the state itself, or with its formal political structures. We can recognise governmentality as being concerned with the exercise of government-type power, and "*the ensemble constituted by the institutions, procedures, analyses,*

[105] Savoie, 2010, p.3
[106] Jessop, 2007, p.39
[107] Collier p.98

and reflections, the calculations and tactics"[108] that allow for the exercise of this power.

In order to perform government, Rose argues[109], strategies and practices are continually developed to link the governing with what they wish to govern. Beyond governance, which concerns the power interactions between actors, governmentality is fundamentally about these strategies and practices driving and enabling the exercise of power by those actors – the rationalities and technologies of power that underpin and inform the power interactions. Gordon argues that governmentality entails a way of "*thinking about the nature of the practice of government … capable of making some form of that activity thinkable and practicable both to its practitioners and to those upon whom it is practiced*"[110]. Looking at power through the lens of governmentality allows us, according to Shore and Wright, to see "*how policies work as instruments of governance, as ideological vehicles, and as agents for constructing subjectivities and organizing people within systems of power and authority*"[111]. Focusing on governmentality – what Foucault termed the "*art of government*"[112] – means that we can conceptualise how power operates and thus locate techniques for the exercise of power within a theoretical framework in which they have an identifiable place, and an identifiable function.

Foucault creates governmentality by linking the two concepts of 'governing' (exercising power) and 'mentality' (the political 'rationality', or set of norms, driving and explaining exercises of power), demonstrating the reciprocal nature of power and knowledge[113]. A particular governmentality involves a variety of technologies of power capable of making a certain space or subject governable and facilitating the 'conduct of conduct', or the exercise of government-type power, in pursuit of a particular goal. It is these technologies that transform

[108] Jessop, 2007, p37 – translating Foucault, 2004a, p.111
[109] Rose, 1999, p.18
[110] Gordon, 1991, p.3
[111] Shore and Wright, 1997, p.35
[112] Lemke, 2001, p.191
[113] Lemke, 2001

ideas and policies into the government-type power interactions that implement them and allow government to be exercised in the manner desired. As discussed previously, it is impossible to talk about power or the technologies involved in its exercise without talking about the underlying rationality. When we talk about a power interaction we must talk about the thought processes and accepted norms that drive and enable its performance. In governmentality, according to Dean, "*government entails any attempt to shape with some degree of deliberation aspects of … behaviour according to particular sets of norms and for a variety of ends*"[114]. In investigating the exercise of power through governmentality we can also investigate the rationalities behind it.

The process by which rationalities are turned by technologies of power into government-type power interactions is known as 'translation'. Rationalities, focusing on the general, are translated into government by the strategies and programmes by which society is rendered governable[115]. As Miller and Rose put it, if rationalities seek to render reality into the domain of thought, technologies of power seek to translate thought into the domain of reality[116]. Without translation government cannot occur – government is a type of power interaction, and without some process that enables the exercise of government-type power there cannot be that interaction regardless of what rationalities are identified. As Rose contends[117], government cannot simply involve a centrally issued order being executed locally. Clearly there must be a process that links ideas and implementation. It was Rose, borrowing from sociology[118], who called this link between the calculations and the practicalities of government 'translation'. In his view, "*in the dynamics of translation, alignments are forged between the objectives of authorities wishing to govern and the personal projects of those organisations, groups and individuals who are the subjects of governance*"[119]. Translation enables government of the governed – the

[114] Dean, 1999, p.18
[115] Rose, 1999, p.48; Jones, 2007, p.174
[116] Miller and Rose, 2008, p.8
[117] Rose and Miller, 1992, p.48
[118] Callon and Latour, 1981, p.286
[119] Rose and Miller, 1992, p.48

influencing of the behaviour of an actor or set of actors in a desired way. A 'governmentality', then, is the combination of rationalities and technologies that are adopted and employed in order to facilitate government-type power interactions through this process of translation.

Care must be taken to avoid the mistake of beginning a governmentality analysis with traditional concepts of the state. Indeed, for Foucault the importance of the state itself was greatly exaggerated. He argued that the state is nothing more than a result of multiple exercises of power[120] – a "*mythical abstraction*"[121] in the study of government. Following from the idea that policies must be turned into government-type power interactions in order to have any effect, Foucault went so far as to say that "*the state is nothing more than the mobile effect of a regime of multiple governmentalities*"[122]. If we are to understand the relationship between citizens (individual actors with agency within the power structure) and the state (an abstraction of the multitude of power interactions between actors within that structure) then we must seek to understand this ensemble. A governmentality analysis allows us to discuss power in a way which rejects a focus on the institutions of state themselves in favour of a wider view. Such an analysis reflects the idea that the state is a construct of numerous governmentalities acting together to create multiple government-type power interactions. Rather than focusing on the formal institutions of state that form the Government, in order to understand the true nature of the power structures that make up the state and the governmentalities that render actors within these structures governable we must focus on government more generally. To this end, we must from this point differentiate between 'government' and 'the Government' – that is to say, we must differentiate between the institutions of the state (Parliament, Cabinet, the courts, etc.) that make up 'the Government', and the wider concept of government (as any government-type power interaction). And just as we must differentiate between 'government' and 'the Government', we must also be

[120] Jessop, 2007, p36
[121] Rose and Miller, 1992, p.2
[122] Jessop, 2007, p36 – translating Foucault, 2004b, p.79

careful to differentiate between 'the state', meaning the complex of public, private, and individual power relations, and 'the State', meaning the formal institutional public state.

We now can say what government is, where it is located, and what it involves. We can conceive of government as the 'conduct of conduct', located where technologies of coercion create a 'contact point' with technologies of the self to produce a desired outcome, and involving technologies of power that seek to translate rationalities into reality and so create a government-type power interaction. We can see that governmentalities are the building blocks of the network of power relationships that together form the illusion of the state, and that the components of these building blocks are rationalities and the technologies for translating those rationalities into reality. When we deconstruct the state to this extent we can examine these government-type power interactions in order to determine the rationalities employed by the actors involved. This allows us to determine the thought processes and norms that drive the exercise of power in these interactions. Identifying these rationalities and technologies through a governmentality analysis is therefore key to an understanding of the relationship between the citizen and the state created through the forms of surveillance-based control to which the digital citizen is subject as a result of the development of new forms of ICT.

2.3 | Digital Citizenship in the Neo-Liberal Mould

Here we seek to establish how the ways that the digital citizen may interact with the digital world can, in neo-liberal societies at least (and in the UK in particular), be seen to fit the neo-liberal mould of the active, self-managing consumer-citizen. As well as facilitating the re-engineering of the citizen-state relationship along active consumer-citizen lines through the provision of services online, contemporary digital citizenship in the UK involves changes in the way that individuals engage with democratic society, furthering the breakdown of traditional party politics into single issue consumer forms, and

also remakes the way that the individual takes responsibility for and manages the self. Digital citizenship in this way has developed in part as a result of the deliberate policies of successive Governments who wish to render the individual amenable to government according to neo-liberal rationalities, and in part as a consequence of the development and emergence of popular forms of ICT in the context of neo-liberal societies.

As noted in Chapter 1[123], the 'digital citizen' for our purposes is any individual who in the course of their daily lives partakes in some way in the modern internet-connected world and 'digital citizenship' as used in this thesis is about with the way in which they go about it. As such, we are not concerned here with any particular conceptions of 'citizenship', but with the way in which the digital citizen has come to engage with the online world, which can be seen to be broadly neo-liberal in nature. We will look at digital citizenship in three ways – first, how the digital citizen interacts with the public sector, then how the digital citizen participates in politics, and, finally, how digital citizens manage the self and their interactions with others

2.3.1 | Digitalisation and E-government

The forms of public service provision in the UK enabled by digitalisation and commonly categorised as 'e-government' can be clearly located within a governmentality framework. Gilritly Nygren describes e-government as "*a term that blurs the borders between public administration, new technology, and changing administrative methods. It has no one definition, but roughly speaking is applied to the processes intended to develop administrative services using a variety of electronic means, and to increase internal efficiency and the public's political influence*"[124]. E-government is itself a governmentality which utilises an array of digitalisation strategies and techniques to bring about a smaller State and render the individual as a digital citizen more amenable to government according to neo-liberal modernising rationalities.

[123] See Chapter 1.1
[124] Giritli Nygren, 2009, p.55

E-government represents a fundamental change in the way that services are provided by the State[125]. Digitalisation, reflecting wider ideals of modernisation drawn from neo-liberal principles, is about 'making up' citizens in the neo-liberal mould by involving them more substantively in their own governance, emphasising citizens actively engaging with the State, citizen choice, and a 'two-way' process of government. E-government requires the individual to take greater responsibility for the self – the citizen becomes the active consumer-citizen in the marketised arena of the public. We have seen how Foucault argued that government lay at the 'contact point' between two kinds of technologies of power – those of the self and those of coercion. E-government moves this contact point closer to the citizen by placing it online, bringing it into computers and other internet-connected devices in people's homes and pockets. Digitalisation thus moves government beyond the traditional confines of the centralised state in which services were provided by the Government in specific locations to which the citizen would have to travel in order to avail of them. In doing so, as digitally-provided services require fewer staff and resources, and despite moving government closer to the citizen, e-government also facilitates a reduction in the size of the State itself in accordance with neo-liberal aims. As Schou and Hjelholt put it, "*Placing the individual at the center of public service means transferring or delegating administrative tasks to citizens rather than governmental personal*"[126]. We can therefore conceptualise e-government – and the policies, systems, and interactions it encompasses – as establishing a new locus for the exercise of government in line with the modernising programmes adopted in the late twentieth century. The governmentality of e-government, then, employs technologies of power to 'make up' the individual as a digital citizen in the neo-liberal mould and render them governable according to neo-liberal rationalities.

In describing this process of making up individuals as digital citizens through e-government, Schou and Hjelholt show that neo-liberal and digital citizenship are becoming intertwined and co-dependent[127]. They examine the Danish

[125] Silcock, 2001, p.1
[126] Schou and Hjelholt, 2017, p.14
[127] Schou and Hjelholt, 2017, p.3

government's digitalisation strategy and argue that neo-liberalisation and digitalisation are mutually reinforcing, and that the development of a digital society has relied on and reproduced neo-liberal forms of citizenship[128]. They describe how the Danish government's strategies seek to render the digital citizen as a neo-liberal subject in several ways. These strategies place, for example, an emphasis on Danish citizens as economically-driven subjects, seeking to maximise both their own productivity and the efficiency of public services[129]. Schou and Hjelholt observe that "*one of the primary objectives of the Danish digitalization strategies has been to transfer the responsibilities from governmental employees, such as social caseworkers and administrative personal employed at the ground level, to the citizens themselves … It also consists in articulating citizens as individualized and responsible for their own circumstances: as agent capable of being active*"[130]. Thus the standard of digital citizenship is set according to neo-liberal principles and the individual is expected to meet that standard. Those who fail to do so are constructed as problematic and undesirable subjects who may be 'digitally illiterate', 'technophobes', or have 'weak IT skills', and who should be corrected through disciplinary measures (education, advertisement campaigns, penalties for performing digital citizenship insufficiently, etc.) in order to bring them up to the required standard[131].

The tax Self-Assessment process provides an example of how digitalisation of a fundamental State function (tax collection) seeks to re-make the role of the citizen in the UK. This encourages eligible individuals to fulfil their annual tax returns through an online system. This includes, for example, individuals who are self-employed, or who have earnings from overseas on which they need to pay tax[132], and there are penalties for failure to comply[133]. Public awareness campaigns for Self-Assessment have used the slogan 'tax doesn't have to be

[128] Schou and Hjelholt, 2017, p.3
[129] Schou and Hjelholt, 2017, p.9
[130] Schou and Hjelholt, 2017, p.13
[131] Schou and Hjelholt, 2017, p.12
[132] For full eligibility details see "Who must send an assessment" at https://www.gov.uk/self-assessment-tax-returns/who-must-send-a-tax-return
[133] See "Penalties" at https://www.gov.uk/self-assessment-tax-returns/penalties

taxing' and emphasise the benefits of using the online system to complete these returns, promoting it as being a convenient option for the individuals who are required to interact with it while at the same time requiring active engagement with the State through ICT and punishing non-compliance. HMRC received 10.24 million Self-Assessment tax returns in the 2014-15 tax year, with 85.5% of these being made using the online system[134]. This represents more than one-third of the total number of UK taxpayers[135], with 210,000 more tax returns filed online than the previous year.

It has been noted[136] that in many countries e-government is still at the 'informational' stage (i.e. citizens are interacting with systems that are primarily focused on "*cataloguing, providing government information by creating government agency Web sites*"[137]) rather than the 'sophisticated' stage (i.e. systems that promote "*transformation, horizontal integration and participation*"[138]). The high engagement rate with the online system is indicative of the fact that policy makers in the UK have been relatively successful in encouraging interaction with the State using ICT, suggesting that e-government here is in the sophisticated stage. While the fact that 14.5% of returns did not use the online system shows that there is a way to go in increasing participation, each of those submitted online represents a separate government-type interaction between the State and the citizen in which individuals have felt compelled by an array of techniques employed by the Government to do as instructed and in which the performance of these instructions is facilitated by digitalisation. In this we can see how ICT and the disciplinary power of the state is employed to reshape the citizen-state relationship as one requiring active participation from the citizen while cloaking this change in the language of choice and convenience by providing online access and bringing the locus of government into the citizen's home.

[134] HM Revenue & Customs, 2015
[135] As per "Table 2.1 Number of individual income taxpayers" available at https://www.gov.uk/government/statistics/number-of-individual-income-taxpayers-by-marginal-rate-gender-and-age - the total number of taxpayers in the 2014-15 tax year was 29.8 million.
[136] Fakhoury and Aubert, 2015, p.346
[137] Yildiz, 2007
[138] Fakhoury and Aubert, 2015, p.346

As Morison describes, e-government policies and practices as employed in the UK have sought to "*re-engineer public services, re-construct ideas of the public, the citizen and the consumer, and govern through these ideas in new market-based citizenship models that privilege consumer power as a means of securing equality and participation through the exercise of choice*"[139]. In truth, promoting online Self-Assessment, and moving government closer to the citizen, means that the Government can close tax offices, reduce staff, reduce expenditure, and cut back the State. We can therefore see the promotion and use of online Self-Assessment as utilising the governmentality of e-government to produce millions of concurrent government-type power interactions facilitated by particular technologies of power (such as digitalisation) in the pursuit of particular rationalities (such as the desire to continue to collect taxes efficiently while reducing the size of the State). E-government assembles systems, ideas, and techniques into one, and this assemblage forms a governmentality that aims to translate general modernising aspirations grown from neo-liberal rationalisations of government into specific outcomes tied to specific programmes. Silcock argues that at the centre of e-government is the customer[140] who, in this case, is the citizen-consumer identified as the subject of neo-liberal governance. Morison concurs, writing that e-government reforms have *"intended to help people not only 'choose' as empowered citizen-consumers but also take part and engage as citizen-participants in shared decision-making as they govern themselves within a wider project of rule*"[141]*.*

Digitalisation, as a technology of power, has allowed individuals to be 'made up' as digital citizens in the neo-liberal mould and so be rendered governable according to the rationalities of the modernised state. Government has moved closer to the citizen (individuals can access services without leaving the house), but conversely the State has shrunk (by being placed online fewer resources are required to provide the service). Rather than services being actively provided to passive citizens, they are passively provided only to active citizens. While it is often emphasised that digitalisation is convenient and empowering for the

[139] Morison, 2010, p.552
[140] Silcock, 2001, p.1
[141] Morison, 2010, p.553

citizen[142], we must recognise that this has the effect of reducing the size of the State, that this is an identifiable trend across many areas of Government policy in the UK, and that this trend can be seen to have been on-going for decades. This reduction in the size of the State in pursuit of the neo-liberal reforming agenda is thus furthered by the use of ICT and the remaking of the individual as a digital citizen. Through this, desires to reinvent the State and to make the public operate more like the private – the rationalities of neo-liberal modernised government – are translated into modernising programmes and specific strategies not only for reforming the State and its interaction with citizens but also for reforming the citizen and their interaction with the State.

2.3.2 | Active Digital Citizenship

In a time where metrics of traditional political participation have been in decline, other forms of participation have taken an increasingly prominent role in public life. Indeed, differences in what is meant by 'political participation' can make a significant difference to how the extent of participation is viewed. Those with a narrow, formal understanding of politics are likely to see a decline in levels of participation, but those with a broader understanding are more likely to see a change in the form of participation[143]. So what do we mean when we talk about political participation? It has often been taken to mean "*those activities by private citizens that are more or less directly aimed at influencing the selection of governmental personnel and/or the actions they take*"[144]. However, this is a narrow definition and excludes attempts to influence the actions of private entities, whether corporations or non-profit organisations, through boycotting and suchlike[145]. We can instead look to the definition formulated by Brady, and understand political participation to mean "*action by ordinary citizens directed toward influencing some political outcomes*"[146]. This

[142] Schou and Hjelholt, 2014, pp.9-11
[143] Hay, 2007, p.71
[144] Verba and Nie, 1987, p.2
[145] Teorell et al, 2007, p.336
[146] Brady, 1999, p.737

encompasses any attempt to influence the actions of governmental personnel as well as those by decision makers in corporations and non-profit entities, so long as those attempts are directed towards a political outcome.

In seeking to conceptualise the factors that enhance or impede political participation, Dahlgren talks about 'civic cultures'[147]. In this he takes the idea that citizens are social agents and asks which cultural factors are behind this agency, looking to determine how they influence and inform the ways that citizens engage politically: "*Civic cultures are potentially both strong and vulnerable: They help to promote the functioning of democracy, they can serve to empower or disempower citizens, yet like all domains of culture, they can easily be affected by political and economic power*"[148]. We can understand that it is within the context of a society that has undergone a neo-liberal revolution over the last few decades, in which the role of the citizen has been dramatically reconfigured as the active consumer-citizen in the marketised public, that people choose whether and how to engage politically online. As Dahlgren acknowledges, "*Market logic, together with emerging legal frameworks and the impetus toward political restrictions, serves to constrain the extent and forms of representation for civic purposes*"[149] .

Reflecting this, much of online political participation takes what Dahlberg calls a 'liberal individualist'[150] form. That is to say that they involve using the internet to provide individuals with the means to access political information and to contact elected representatives directly[151]. The trend towards choice-making and active citizenship promoted through neo-liberalisation can be seen in the forms online political participation that are facilitated by the internet and promoted online. These are largely a consumer form of politics where the digital citizen can pick and choose among single-issue campaigns being offered as commodities in the marketised public and is imbued with responsibility for

[147] Dahlgren, 2005, p.157; see also Dahlgren, 2003
[148] Dahlgren, 2005, p.158
[149] Dahlgren, 2005, p.151
[150] Dahlberg, 2001, p.618
[151] Dahlberg, 2001, p.618

contacting politicians and decision-makers directly, creating a form of active digital citizenship. As Dahlberg argues,

> *"liberal individualist political initiatives share an emphasis upon information provision and direct communication between individuals and decision makers. This emphasis assumes a political subject who only needs to be given the appropriate information in order to make the right choices. This subject suits governments and corporates because it fits a top-down consumer model of politics where individuals choose from an array of competing political positions displayed before them"*[152]

Websites such as TheyWorkForYou[153] and WriteToThem[154] provide information on the voting records of elected representatives and transcripts of their speeches in Parliament, in the European Parliament, in the devolved legislatures, and in local councils, as well as information on their expenses claims, social media contact information, and methods by which individuals can contact their representatives directly using online forms of communication facilitated by those sites. And, e-petitioning systems, both official (such as https://petition.parliament.uk or https://petitions.whitehouse.gov) and unofficial (such as https://www.change.org and https://38degrees.org.uk), provide ways for citizens to contact decision makers in government as well as in corporations and non-profit organisations. Individuals are asked to sign and share e-petitions created by an array of activist groups (or by private companies such as Uber, which uses e-petitions to put pressure on governments who are considering regulating or banning its service[155]). The digital citizen is thus presented with an array of options where issues and campaigns are offered to them as commodities, and, just as the consumer is tasked with choosing the products they wish to purchase in a supermarket, is tasked with making an informed choice of which campaigns to support. Links to these e-petitions and

[152] Dahlberg, 2001, p.620
[153] https://www.theyworkforyou.com
[154] https://www.writetothem.com
[155] Ranchordas, 2017

other forms of consumer political action may be widely shared in online spaces, and as a result may attract large audiences (an e-petition which sought a second referendum on the UK's membership of the EU, for example, received more than four million signatures[156] after being widely shared on social media, while a petition requesting that the Government cancel a proposed state visit by Donald Trump received nearly two million signatures[157]). As of 2017, 23% of the British public say that they have signed an e-petition in the last 12 months and 36% say that they would do so[158]. While still low compared to the proportion of the public who have voted in the last year (57%), participation through e-petitioning is on an upward trend – since 2013 the proportion of the public who have signed an e-petition in the previous 12 months has increased by 14 points (from 9%)[159]. Change.org strongly encourages those who sign e-petitions on its website to take an active part in the campaign by sharing the petition on social media, and provides links and suggested text for doing so.

But it is not just through obviously liberal individualist forms of activism that the digital citizen participates in politics. Graham et al discuss how websites act as incubators of political action, creating everyday public spaces[160]. They look at places that are formally non-political –which are not intended for political purposes – where people interact informally and where political talk, organising, and action can organically develop as users make connections between their everyday experiences and contemporary social and political issues[161]. Graham et al note that in a time of austerity in the UK, where individuals are increasingly expected to fend for themselves and public services are cut back or contracted out as the State is reduced in size, these kinds of online spaces have grown in prominence as people take a greater role in actively managing their lives and their relationship with civil society[162]. Their research shows that not only do people involved in these spaces routinely seek

[156] https://petition.parliament.uk/archived/petitions/131215
[157] https://petition.parliament.uk/archived/petitions/171928
[158] Hansard Society, 2017, p.43
[159] Hansard Society, 2013, p.38
[160] Graham et al, 2015
[161] Graham et al, 2015, pp.1-2
[162] Graham et al 2015, p.2

and give advice and support on dealing with government and civil society on a personal level[163] – for example, on how to obtain social housing or a crisis loan, how to manage personal debt, or how to navigate the bureaucracy of public services – but also that such conversations can (in 68% of studied cases) spawn broader political discussions[164] that may go on to encourage action on a more general level[165]. These include, for example, joining or organising a campaign or protest, boycotting and consumer activism, and signing or creating a petition[166]. And these kinds of participation are increasing in popularity – as of 2017, 10% of the British public say that they have taken part in a boycott in the last 12 months (a further 25% say that they would do so in future), and 9% say that they have taken part in an online political discussion in the last 12 months (19% say that they would do so in future)[167]. Since 2013 these numbers have increased by 4 points (from 6%) and by 6 points (from 3%)[168], respectively. At the same time the online world has facilitated the creation of spaces in which members of historically marginalised groups to gather and discuss commonalities. These spaces offer support, advice, and community, and may also provide other opportunities. Baker et al[169], for example, looked at how disabled and elderly people use social networking sites to form community groups, and found that the members of these groups use social networks for community participation – as may be expected – but also for political action and civil engagement[170].

While online spaces may be seen as facilitating somewhat more communitarian participation, co-ordinating campaigns and bring people together for common purposes, in terms of the political action they foster it is often single issue in nature, again reflecting consumer forms of politics, and in many cases they do little more than provide guidance on how individuals can contact politicians or

[163] Graham et al, 2015, pp.7-8
[164] Graham et al, 2015, p.8
[165] Graham et al, 2015, p.11
[166] Graham et al, 2015, p.10
[167] Hansard Society, 2017, p.43
[168] Hansard Society, 2013, p.38
[169] Baker et al, 2013
[170] Baker et al, 2013, pp.29-32

engage with the State and civil society directly themselves. As such, the digital citizen ultimately still fulfils a largely liberal individualist role (and even boycotting, a form of collective rather than individual action, is politics through consumer choice-making[171]). This is a product of the neo-liberal civic culture in which these spaces develop in the UK. The need to seek help with navigating the neo-liberal state as an active consumer-citizen combined with forms of online communication and interaction results in digital citizens organically discussing the social and personal issues that they encounter in their everyday lives, making connections between those issues and Government policies, and organising politically against the effects of neo-liberalism itself, but doing so in a way that's fundamentally neo-liberal in nature.

The internet thus contributes to an ongoing neo-liberalisation of participatory democracy and of politics, facilitating a marketization, commercialisation, and commodification of politics. As a result, the role of the digital citizen as a political agent in these spaces is fundamentally neo-liberal in nature, reflecting that of the active consumer-citizen of the neo-liberal ideal operating in a marketised public.

2.3.3 | Digital Self-Management

In contemporary society individuals are expected to construct their own lives and encouraged to take responsibility for themselves[172]. Individualisation is central to self-hood and citizenship in neo-liberalism, which, as discussed previously, in theory prioritises the sovereign individual as the key component of society, imbued with personal responsibility and engaged in self-management in the pursuit of self-interest. Self-management forms the self-directed element of personal responsibility alongside societally-directed active consumer-citizen, which in a governmentality framework can be located as those technologies of the self that are concerned with managing the self. In our analysis of digital citizenship this can broadly be divided into two categories –

[171] Stole et al, 2005; Teorell et al, 2007
[172] Beck and Beck-Gernsheim, 2001; Bauman 2007, pp.58-59

the first, digitally managing the self, concerns using digital tools to manage life and health; the second, managing the digital self, concerns privacy, identity, and representation of the self in the online world.

Digitally Managing the Self

An important aspect of neo-liberal citizenship is that the individual takes personal responsibility for the management of their own physical self, and recent developments in ICT have made this possible in new ways. These include, for example, devices such as fitness trackers and health monitoring wristbands, as well as apps to measure sleep quality, to record calorie intake, to monitor medication use, and so on. 'Smart' objects forming part of the Internet of Things have also been developed, allowing individuals to monitor driving habits and drowsiness, for example[173]. Self-tracking devices or apps will often set goals or targets for the user to meet, such as a recommended calorie intake (sometimes tailored to achieve a certain level of weight loss) or an apparently beneficial level of physical activity (such as walking 10,000 steps per day[174]). Self-tracking allows users to track and quantify all aspects of their lives[175], helping them to measure and manage their behaviour[176]. Individuals are often encouraged to engage in self-tracking[177], whether by the companies who offer these services as they promote their benefits, by organisations promoting health and fitness, or, for example, by car insurance companies who promise lower premiums if a driver allows their driving to be tracked.

Part of this process is the datafication of health, fitness, and daily activity, or what Charitsis calls 'self-quantification': "*self-quantification aspires to enhance human abilities through self-knowledge, by collecting and analyzing data for everything related to the human body and mind that can be measured*"[178]. The

[173] Lupton, 2014
[174] Goodyear et al, 2017, p.3
[175] Charitsis, 2016, p.38
[176] Dennison et al, 2013; see, e.g., Lupton, 2015; Lupton, 2013
[177] Lupton, 2013; Lupton, 2014; Goodyear et al, 2017
[178] Charitsis, 2016, p.45; see also Lupton, 2016

'quantified self' has become a popular term to describe this self-tracking[179]. Shilton describes it as 'participatory personal data', or "*aggregations of representations or measurements collected by people, about people*"[180]. According to Shilton, these are participatory in that data is collected with the intention that it will be available to the individual themselves[181], a form of self-surveillance by which the digital citizen makes use of ICT in order to manage the real-world self[182].

This facilitates the increasingly detailed measurement and monitoring of people's lives, bodies, and behaviours[183], and fits the neo-liberal drive to quantify all aspects of life so as to render them thinkable, knowable, and therefore governable[184]. And setting a goal for a user to attain establishes a behavioural norm for the individual to meet. This process of normalisation was identified by Foucault as being central to neo-liberal forms of government[185], whereby standards of ideal behaviour are established and the individual is held to that standard. Self-tracking can also be located as a form nudging[186], a method of control put forward by Thaler and Sunstein[187] that can be located in the neo-liberal tradition whereby responsibilities are placed onto individuals. We can further locate self-tracking as a form of the algorithmic regulation described by Keren Yeung[188], in this case an individual seeking to regulate the self. And in our governmentality analysis we can recognise self-regulation through self-tracking as a technology of the self which is used in line with neo-liberal concepts of citizenship and the role of the individual within society[189]. Through this, self-tracking seeks, as Miller and Rose describe the governmentalities of neo-liberalism, "*to act upon and instrumentalize the self-regulating propensities of individuals in order to ally them with socio-political*

[179] Lupton, 2016
[180] Shilton, 2012, p.1906
[181] Shilton, 2012, p.1907
[182] Lupton, 2013, p.395
[183] Lupton, 2014
[184] Miler and Rose, 1990
[185] Foucault, 1991
[186] Galič et al, 2017, p.30; Lupton, 2016, p.107
[187] Thaler and Sunstein, 2008
[188] Yeung, 2017
[189] Foucault, 1988; Lupton, 2014, p.12

objectives"[190], and reflects the emphasis in neo-liberal theory placed on the citizen as a self-managing, sovereign individual, ultimately responsible for their own health and lifestyle[191].

Self-tracking of the kind identified here therefore helps manage the behaviour of the digital citizen and renders them self-governable according to modernising, neo-liberal norms, with the idea of perpetual self-management in everything from personal fitness to car insurance becoming normalised[192]. And as well as the use of digital technologies to manage the physical self, the digital citizen also uses a variety of techniques to manage the digital self. We will move on to discuss this now.

Managing the Digital Self

Digital life requires the active managing of social relationships. It is no longer enough to maintain a sporadic friendship with someone in the era of social media, instead the individual is expected to continually take part in a wide range of online forms of social interaction – from 'liking' or commenting on photos and statuses posted by friends, to uploading their own content, posting statuses, and so on. Social life becomes something to be actively managed in much the same way as any other aspect of life. There are two inter-related aspects to this: privacy management and identity management. We will deal with each of these in turn.

We begin with what Daniel Solove calls 'privacy self-management'[193], where individuals are largely held to be responsible for managing their own privacy and security online. This places responsibility for privacy violations firmly with the individual, as would be expected in neo-liberalism. Users have developed a variety of strategies to manage their online privacy[194]. They may, for example,

[190] Miller and Rose, 1990, p.28
[191] Lupton, 2013; Rich and Miah, 2017
[192] Lupton, 2014, p.12
[193] Solove, 2013
[194] Lankton et al, 2017; see also Bartsch, 2016; Moll et al, 2014

limit self-disclosure[195], make use of the privacy settings provided by various platforms[196], or control the size of their network or friend list. They may, to a greater or lesser degree, perform some combination of the three[197]. Users may target what they post to the 'lowest common denominator' – i.e. if their friends on social media include a combination real friends, family, and colleagues then they may self-censor so as to post only benign content intended to avoid offence or controversy among members of all of those groups in order to avoid disapproval[198]. Some users may post more personal or contentious information but make use of privacy settings to limit the audience for each post, so as to effectively disclose different things in different social settings[199]. Research has shown that users actively engage with privacy and security settings on social media, managing their exposure to risk by taking precautions according to their perception of risk[200], and where a particular setting is perceived to address a greater risk users are more likely to make use of it[201]. This means that users consider the implications of privacy management behaviours and take steps accordingly, although navigating privacy settings – which differ across platforms – may require a degree of knowledge about the platforms themselves in order to be operated most effectively. And Raento and Oulasvirta found that in many cases users aren't concerned so much with protecting their privacy per se as they are with presenting themselves appropriately in different situations and contexts[202].

Privacy self-management thus forms part of online identity management, where the choice of what to share or not to share, which is often informed by privacy concerns[203], forms part of the process of developing and maintaining an online identity (usually manifested through a user profile). As van Zoonen observes, cultural and social theories of identity hold that it is not just something that we

[195] Nosko et al, 2010; Stutzman et al, 2011
[196] Bartsch and Dienlin, 2016
[197] Lankton et al, 2017, pp.150-151
[198] Lankton et al, 2017, p.155
[199] Kramer and Haferkamp, 2011; Lankton et al, 2017, p.155
[200] van Schaik et al, 2018
[201] van Schaik et al, 2018, p.294
[202] Raento and Oulasvirta, 2008, p.529
[203] Krasnova et al, 2010; Zlatolas et al, 2015; Ranzini and Hoek, 2017

are, but something that we *do*[204]. On the internet, as is the case elsewhere, identity is constructed and performed[205]. Users on social media will often have to decide whether, accounting for privacy and other factors, it is prudent to share a particular photo or a particular piece of information about themselves[206]. Self-expression on social media therefore in large part involves a 'risk versus reward' calculation[207], whereby the choice of what to post online is made with conscious awareness of privacy implications, of the intended audience, and of the image that they hope to present to others[208]. Individuals engage in a process of self-monitoring when presenting themselves online[209], just as they do offline[210]. Will a particular photo convey them in the desired way? Will a particular comment divulge information about them that they do not wish to be made public? Is a particular post something that they would want their family or employer to see, or should it be limited only to their real-world friends? These kinds of questions, and many more, are routinely considered as part of self-monitoring and self-performance on social media[211]. Someone who visits both an art gallery and a bar in the same day may choose to 'check in' at the former rather than the latter (or vice-versa) so as to present a particular version of themselves according to the identity that they wish to perform, for example. And research into the behaviour of teens on Facebook shows that they actively manage their profiles in order to manage the way that they present themselves[212].

This process of determining how to present oneself to whom is one by which users "*present a highly curated version of themselves*"[213]. In the online world, user profiles, such as those on Facebook, for example, stand in for the real person as '*data doubles*' of the real person[214]. These profiles are digital

[204] van Zoonen, 2013 – see, e.g., Goffman, 1956; Butler, 1988
[205] van Zoonen, 2013; see also Schwartz and Halegoua, 2015
[206] Rosenberg and Egbert, 2011
[207] Besley, 2010, pp.130-131; Davis, 2011
[208] Ranzini and Hoek, 2017
[209] Rosenberg and Egbert, 2011
[210] Snyder, 1974
[211] Davis, 2011
[212] Madden et al, 2013, pp.8-9
[213] Schwartz and Halegoua, 2015, p.1645; see also Mendelson and Papacharissi, 2010
[214] Heggarty and Ericson, 2000

representations of the self that provide a window into the personality of the individual. And the way that each user chooses to portray themselves through their social media profiles is itself a form of active self-management where users are managing their digital selves. The ongoing process of profile curation – for example, choosing a profile picture, choosing what posts to make public, choosing which photos to upload, and choosing what information to share about yourself in terms of your age, gender, religious beliefs, political views, work, education, and relationships – is an online manifestation of the self-management in which the neo-liberal citizen is expected to be engaged.

Many individuals – including teenagers, young adults, and professional adults of all ages – shape their online identities with the goal of gaining popularity with, recognition from, and connection to peers, colleagues, and potential employers[215]. Thus identity self-management on social media can also be understood as self-commodification, as Bauman describes:

> *"The schoolgirls and schoolboys avidly and enthusiastically putting on display their qualities in the hope of capturing attention and possibly also gaining the recognition and approval required to stay in the game of socializing … are enticed, nudged or forced to promote an attractive and desirable* commodity*, and so to try as hard as they can, and using the best means at their disposal, to enhance the market value of the goods they sell. And the commodity they are prompted to put on the market, promote and sell are themselves.*
>
> *They are, simultaneously,* promoters of commodities *and* the commodities they promote*"*[216]

[215] van Dijck, 2013, pp.202-203
[216] Bauman, 2007, pp.5-6

Curating a Facebook profile is therefore commodification of the self of the kind identified by Bauman as being central to the modern consumerist society[217]. As he puts it, "*The most prominent feature of the society of consumers – however carefully concealed and most thoroughly covered up – is the* transformation of consumers into commodities"[218]. In the marketised neo-liberal state, as part of the need to self-manage, the digital self therefore becomes a commodity to be actively promoted in the social and employment markets. As part of the need to actively manage online identity and engage in social and professional relationships online, the digital citizen is thus involved in both self-commodification (turning the self into a commodity by creating and curating a profile representing that self) and also self-promotion ('selling' that commodified self to others)[219].

Self-commodification is an ongoing, perpetual process, but it isn't entirely of the digital citizen's own doing. Through the process of profile curation, the information that each website asks of users and prioritises for the purposes of completing and displaying their profile shapes the way that identity is constructed in those spaces[220]. Facebook profiles reflect its emphasis on social activity and personal relationships, whereas LinkedIn promotes the creation of a profile centred on education and employment history, professional achievements, and business-related networking[221]. van Dijck argues that the influence that sites hold over the creation of online identity means that identity self-management becomes directed towards corporate ends:

> *"[user profiles] are not a reflection of one's identity, as Facebook's Marc Zuckerberg wants us to believe, but are part and parcel of a power struggle between users, employers/employees and platform owners to steer online information and behaviour"*[222]

[217] Bauman, 2007, p.6
[218] Bauman, 2007, p.12
[219] Rosenberg and Egbert, 2011
[220] Kimmons, 2014, p.95
[221] See van Dijck, 2013
[222] van Dijck, 2013, p.212

These sites thus guide the construction of the online identity of their users, tailoring it to the purpose envisaged by and in line with the values of the sites themselves[223]. But this also means that individuals can use each site to present a different aspect of their identity for a different audience, actively managing the performance of their selves across multiple platforms, and self-commodifying in a different way in different contexts. We can adopt our governmentality analysis to identify the various ways that sites encourage users to present themselves – whether by prompting for particular information, by algorithmically promoting certain information, and so on – as technologies of power that shape self-commodification by users in line with corporate goals (which we can recognise as rationalities). They exercise this form of government at the contact point of these technologies and of the technologies of the self and in doing so encourage the selective, context-specific sharing of information that constitutes self-management of digital identity.

Through privacy self-management as part of identity management and self-commodification the digital citizen is engaged in the self-management required of the individual in neo-liberal societies, facilitated by ICT. Along with the remaking of the relationship between the citizen and the State through the governmentality of e-government and the increasingly neo-liberalised form of active citizenship in the political sphere, we can identify this as a key aspect of the emergence of a neo-liberal form of digital citizenship.

2.4 | Conclusion

In this chapter we have set out the key points of neo-liberal theory, and shown how reform has been pursued by framing it as being in the best interests of society as a whole in disciplinary neo-liberalism. Neo-liberalism prioritises the free market, a smaller state, and the sovereign individual imbued with personal responsibility for all aspects of their lives as the self-managing consumer-citizen

[223] Kimmons, 2014, pp.95-96

actively engaged in civil society. This brings a shift from nation state to market state and requires the revolution described in governance theories, with the shrinking of government, privatisation of the public, and an emphasis on self-government by the citizen representing a significant shift away from the welfare state.

Concepts of governance and governmentality can explain how government in neo-liberal societies functions, and provide us with a theoretical framework for discussing the forms of power and control to which the digital citizen is subject in the online world. With this governmentality framework we can now conceive of the state, power, and government in such a way as to allow us to determine why, how, and where it is exercised. As we have seen, government, as the conduct of conduct, is located at the 'contact point' of two kinds of technologies of power – where technologies of the self and technologies of coercion combine to govern conduct.

We have also seen how digital citizenship has itself developed along neo-liberal lines, reflecting the fact that the emergence of the internet as a significant factor in society has taken place alongside the revolution in British government and society that the neo-liberal reforming project represents. We can understand the digital citizen as a sovereign, self-managing consumer-citizen, imbued with personal responsibility for all aspects of their life and tasked with exercising their agency through the technologies of the self as a social, economic, and political actor in pursuit of their own self-interest. Successive governments in the UK have adopted the governmentality of e-government to encourage individuals to interact with a smaller, hollowed-out State online, reflecting the move of all aspects of life towards the digital. Online forms of consumer politics have resulted in the individual operating as an active digital citizen in the new marketised public, choosing from an array of commodified issues and campaigns in liberal individualist varieties of political engagement. The individualised digital citizen manages their physical body through the technologies of the self which are enabled by digital self-tracking. They also manage the digital self in the ongoing processes of privacy and identity

management through their technologies of the self, shaped by the technologies of coercion of corporations who are pursuing their own rationalities, resulting in the self-commodification of the individual in digital form as expected in contemporary marketised society.

These conceptual foundations will allow us to develop the central argument of this thesis. We can recognise the neo-liberal characteristics of digital citizenship, and governmentality gives us a framework within which we can locate and define power, government, and the state and with which we can discuss the forms of control to which the digital citizen is subject – the governmentalities, with their rationalities and technologies of power, that exist in the digital world. As we shall see in subsequent chapters, this neo-liberal form of digital citizenship renders the individual more amenable to surveillance-based governmentalities involving commercial, security, and political rationalities which remake the relationship between the digital citizen and corporations, the State, and political organisations to the detriment of the digital citizen. We will now move on to examine the first of these – the commercial rationalities of surveillance capitalism, and how corporations involved in this new business model exercise control over the digital citizen through the technology of power of algorithmic governmentality.

Chapter 3 | Commodifying Life: Surveillance Capitalism and the Digital Citizen

> *"Google is ground zero for a wholly new subspecies of capitalism in which profits derive from the unilateral surveillance and modification of human behavior. This is a new surveillance capitalism that is unimaginable outside the inscrutable high velocity circuits of Google's digital universe"*[1]
>
> - Shoshana Zuboff

So far we have seen how in the UK the state has developed along broadly neo-liberal lines since late 1970s, bringing a marketization of the public and civil society and a remaking of the individual as an active consumer-citizen, and have identified the emergence of a digital form of citizenship in this mould with the growing influence and prevalence of ICT and online life. We will now look at how this increasingly digital modern world has opened the digital citizen up to new forms of dataveillance-based control by corporations, who seek to commodify modern life in the pursuit of profit. And we will see that this involves a new relationship between corporations and digital citizens, as individuals are commodified as data profiles and their agency is appropriated and turned against them for profit.

In 2015, Shoshana Zuboff identified the emergence of a new form of capitalism, created by Google through its use of big data in much the same way as Ford lead the way in mass production and General Motors pioneered managerial capitalism a century earlier. In doing so Zuboff described big data not as a new

[1] Zuboff, 2016

technology itself nor an inevitable and unavoidable consequence of technological progress, but as a "*foundational component"* in a new business model that "*aims to predict and modify human behavior as a means to produce revenue and market control*"[2]. She calls this new model 'surveillance capitalism'[3], with gathering and analysing as much data as possible at its core, seeking to predict and influence user behaviour in order to induce desired behaviours from which profit can be generated. Ultimately, surveillance capitalism involves commodifying as much as possible of everyday life in the pursuit of profit. Zuboff makes a largely business- and economics-orientated argument and makes little reference to the surveillance studies literature. In this chapter, surveillance capitalism will in part be located within that and other literature with the aim of contextualising and further fleshing out some of her ideas, intending to expand on what surveillance capitalism means for the digital citizen.

Andrejevic observes that an analysis of big data that takes the form only of a critique of privacy invasion "*does not do justice to the productive character of consumer surveillance*"[4]. Looking at the implications for power and control is necessary in order to produce a fuller picture of what this means for the digital citizen in the modern world – as Andrejevic says, "*the prospect that advertising might become more effective because it will be able to predict human behaviour with a high degree of reliability and thereby manage the populace more efficiently in accordance with commercial imperatives is disturbing in a different way from privacy concerns*"[5]. The rationality and technology of power of surveillance capitalism, the role of the individual in surveillance capitalism, and the possibility of resisting surveillance capitalism are therefore essential topics for discussion.

As such, this chapter will set out the origins of surveillance capitalism and adopt the governmentality analysis set out in Chapter 2 to identify and describe its

[2] Zuboff, 2015, p.75
[3] Zuboff, 2015
[4] Andrejevic, 2012, p.73
[5] Andrejevic, 2012, p.73

rationality and technology of power; then we will look at what this means for the digital citizen in terms of their role within that system and the implications for individual sovereignty in the neo-liberal ideal; and will discuss the prospects for resistance in the age of surveillance capitalism. In all, we will identify and account for the relationship between the digital citizen and the corporations involved in surveillance capitalism, and will locate surveillance, predictive algorithmic analysis, and associated developments as a technology of power that translates the rationality of surveillance capitalism into reality by remaking the digital citizen as an individual amenable to its control.

3.1 | The Reality Business

We will first set out the business model identified by Zuboff and put forward its underlying rationality, before moving on to identify the technologies of power involved in surveillance capitalism and examine how they operate through the algorithmic analysis of user data to translate this rationality into reality by predicting and influencing human behaviour.

3.1.1 | The New Surveillance Capitalism

Zuboff grounds her analysis in two articles written by Google's Chief Economist, Hal Varian, on big data[6] and computer-mediated transactions[7], which broadly set out the principles behind Google's business model. Computer mediation will first be discussed, describing what it is and how has been utilised in this business model, and surveillance capitalism will then be identified as a new form of capitalism involving the computer mediation of big data with an underlying logic of accumulation that we can identify as its new rationality.

[6] Varian, 2014
[7] Varian, 2010

Informating through Computer Mediation

Zuboff herself laid the groundwork for theoretical discussions around computer mediation, first in 1981[8] and through her subsequent work. She recognised that computers not only have the capacity to automate tasks, as was the case with previous technologies created to replicate or reduce human labour, but also to 'informate'. This means that automation by computers, unlike automation by mechanical devices such as the weaving loom of the first industrial revolution, also produces information that is new and otherwise unknowable, leading to greater understanding of things which had previously been opaque[9]. Zuboff contrasted the 'dumb' mechanical devices of previous technologies, which can only automate, with 'smart' computers that can informate[10]. As Zuboff notes, informating through computer mediation has become part of everyday life as it is increasingly rendered in the digital dimension, meaning that events, objects, processes, and people become "*visible, knowable, and shareable in a new way*"[11].

Informating through computer mediation of big data can provide a wealth of otherwise unknowable information to companies involved in surveillance capitalism. Research into what information Facebook Likes can disclose about an individual when analysed provides a good example of how computer mediation can provide insight into personal lives from relatively impersonal behavioural data[12]. Analysis of Likes has been shown to accurately predict various sensitive personal attributes including sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The accuracy of such prediction is in some cases very high – the analytical model employed by the researchers in the study of Likes can correctly distinguish between homosexual and heterosexual men in 88% of cases, between African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in

[8] Zuboff, 1981
[9] Zuboff, 1988
[10] Zuboff, 1988, p.395
[11] Zuboff, 2015, p.76
[12] Kosinki et al, 2013, p.5802

85% of cases. This kind of information can be fed into predictive models in order to enable companies to more accurately target prospective customers and to more effectively guide them towards the desired behaviour.

Utilising Computer Mediation

Google provides the prototypical model of how informating through computer mediation of data gathered through surveillance of online behaviour can provide otherwise unknown information which can be used to predict and influence future behaviour in order to produce profit. In using Google search we provide Google with behavioural data, such as the queries that we enter into the search box. For Google this data is essentially a cost-free by-product of our use of their services, what Zuboff calls 'behavioural surplus'[13], and is collected without much effort or even awareness on the part of those being surveilled[14]. Varian tells us that Google's co-founder Larry Page used to say that Google's problem was that users had to ask it questions – *"He thought Google should know what you want and tell it to you before you ask the question*"[15]. By gathering the behavioural data produced by users and subjecting it to algorithmic analysis Google is able to predict what users are going to type and offer auto-complete suggestions for searches. They can then provide targeted advertising on the search results page based on the predicted likelihood of users who have entered similar search terms and who fit similar user profiles, again determined by predictive analysis, to follow particular links or prompts.

It is this ability to use the information produced by computer-mediating behavioural data to predict future user behaviour that enables Google and similar companies to attempt to influence that behaviour. And the same principle has been applied beyond search. For example, through the Google Now smartphone app, Google can constantly provide users with information that it predicts will be relevant to them at any given point in time or in any given

[13] Zuboff, 2016
[14] Mayer-Schoenberger and Cukier, 2013, p.101
[15] Varian, 2014, p.4

location in order to prompt users to engage with Google's targeted services and advertising. Google sells space for targeted advertising both within their own services and on other websites, which receive a share of the revenue from that advertising, to other companies for profit. Google itself determines which adverts and prompts should be shown when, where, and to whom. As such, over the past two decades Google has derived substantial profit from the computer mediation of behavioural data, first by using it to sell targeted advertising in search, then by surveilling and datafying behaviour elsewhere so as to predict and modify future behaviour more generally and maximise opportunities for profit in many other contexts. This is how Google, which began in Page and co-founder Sergey Brin's shared dorm room at Stanford University in 1995, went from being an unprofitable internet search engine in the 1990s to being a vastly profitable advertising company in the 2000s and one of the biggest companies in the world in the 2010s. In doing so it invented the business model broadly followed by the companies that dominate the new digital world. This model underpins what Zuboff calls the 'reality business' – "*a new business frontier comprised of knowledge about real-time behavior that creates opportunities to intervene in and modify behavior for profit*"[16].

Computer mediation of the behavioural data produced by our use of online services with the result of both automated and informated outputs is therefore central to surveillance capitalism. And as our lives are increasingly digital they are increasingly computer-mediated, rendering us as digital citizens visible, knowable, and amenable to control.

The Rationality of Surveillance Capitalism

Zuboff sets out the component parts of surveillance capitalism – what she calls its 'equation'; what we can recognise as its *rationality* – as follows:

[16] Zuboff, 2015, p.84

> *"First, the push for more users and more channels, services, devices, places, and spaces is imperative for access to an ever-expanding range of behavioral surplus. Users are the human nature-al resource that provides this free raw material. Second, the application of machine learning, artificial intelligence, and data science for continuous algorithmic improvement constitutes an immensely expensive, sophisticated, and exclusive twenty-first century 'means of production.' Third, the new manufacturing process converts behavioral surplus into prediction products designed to predict behavior now and soon. Fourth, these prediction products are sold into a new kind of meta-market that trades exclusively in future behavior. The better (more predictive) the product, the lower the risks for buyers, and the greater the volume of sales. Surveillance capitalism's profits derive primarily, if not entirely, from such markets for future behaviour"*[17]

There should be little doubt that, as Zuboff puts it and has been noted by others, including Google's former Engineering Director James Whittaker[18], "*Google's business is the [advertising] auction business and its customers are advertisers*"[19]. The advertising market is the 'meta-market' identified by Zuboff. For Google, the digital citizen is a user, rather than a customer, and we are the source of the raw material of surveillance capitalism, to be auctioned to highest bidder – not just personal data, but the computer-mediated behavioural surplus produced by the digital citizen as they move through the digital world. Through computer mediation of the daily life of the digital citizen, surveillance capitalism renders their lives visible, knowable, and profitable to corporations.

This represents a break from previous forms of capitalism. While in industrial capitalism profit derived from the production of goods, and in financial capitalism profit derives from speculating on the future value of financial

[17] Zuboff, 2016, p.6
[18] Whittaker, 2015
[19] Zuboff, 2015, p.78

instruments, in surveillance capitalism profit derives from the surveillance and modification of human behaviour[20]. Consequently, while in industrial capitalism power derived from control of labour and ownership of the means of production, in surveillance capitalism power derives from surveillance and computer mediation[21]. This moves surveillance capitalism away from the analysis of scholars such as Fuchs, who has argued that Marx's cycle of capital accumulation – in which labour power and the means of production are purchased in order to produce new commodities in the expectation of making a profit, some of which may be reinvested thus continuing the cycle – can be applied to other forms of surveillance[22], including the early neo-liberal consumer surveillance identified by Stephen Gill[23], to show how surveillance is a device for extending power in that cycle. Fuchs himself does acknowledge this, and has put forward his own interpretation of Google's business model which is grounded in Marx's theory but rightly departs from it[24]. But in this he does not account either for the role of predictive algorithmic analysis as a new means of production in converting behavioural data into prediction products or for the role of behaviour modification within that business model, so does not identify its key aspects and thus in that sense does not go far enough in distinguishing this new form of capitalism from what has gone before.

The new cycle of capital accumulation of surveillance capitalism, which we can identify as its rationality, does not fit the industrial model of accumulation, nor does it fit the model of financial capitalism that has been central to the global economy for decades. It moves beyond past and present forms of capitalism – as well as past and present analyses of capitalism, such as that provided by Marx and built upon by Fuchs – into something new, with surveillance standing not just as a technology of power in the existing order but becoming the defining

[20] Zuboff, 2016
[21] Yeung, 2017a, p.130
[22] Fuchs, 2012
[23] Fuchs, 2012, pp.681-682; Gill, 1995
[24] Fuchs, 2011; Fuchs is by no means the only writer to apply Marxian perspectives to ICT generally (see, for example, Dyer-Wytheford, 1999 and Dyer-Wytheford, 2015). But, although Galič et al. refer to surveillance capitalism as described by Zuboff as "*(neo-) Marxist surveillance theory*" (2017, p.24), few other than Fuchs have attempted to apply such an analysis to explain surveillance capitalism, specifically.

feature of a new order, at the heart of a new logic of accumulation. As Zuboff says,

> *"This is how in our own lifetimes we observe capitalism shifting under our gaze: once profits from products and services, then profits from speculation, and now profits from surveillance"*[25].

Having distinguished surveillance capitalism from previous forms of capitalism, it is necessary at this point to also distinguish surveillance capitalism from the 'platform capitalism' described by Srnicek[26], Pasquale[27], and others[28]. This involves corporations extending their reach through the creation of platforms:

> *"At the most general level, platforms are digital infrastructures that enable two or more groups to interact. They therefore position themselves as intermediaries that bring together different users: customers, advertisers, service providers, producers, suppliers, and even physical objects. More often than not, these platforms also come with a series of tools that enable their users to build their own products, services, and marketplaces"*[29]

Advertising platforms are one of the five types of platform identified by Srnicek[30], and he acknowledges surveillance capitalism within that category. But while not all platforms are surveillance corporations (platforms typically do extract and analyse personal and behavioural data, but this is not necessarily for use in a surveillance capitalist mode of profit-making), it is also the case that not all surveillance corporations are platform corporations. However, there is significant overlap. In particular, Google, Facebook, and Amazon, three of the leading proponents of surveillance capitalism (or, in the case of Amazon, a variant thereof), are clearly platform corporation; their presence stretches

[25] Zuboff, 2016, p.6
[26] Srnicek, 2016
[27] See, e.g., Pasquale, 2017
[28] See, e.g., Olma, 2014; Langley and Leyshon, 2017
[29] Srnicek, 2016, p.43
[30] Srnicek, 2016, p.50

across the internet and they provide products and services far beyond their original iterations of search, social media, and selling books. But smaller companies, which make use of broadly the same business model, do not necessarily take the form of a platform.

In order to reconcile these two concepts, we can distinguish between the organisational characteristics and the profit-making characteristics of any particular corporation (the two are of course linked, but the distinction, while blurry, is a useful one to make for our purposes). Organisational characteristics are those which describe the form of organisation that the corporation takes as it seems to maximise opportunities for profit, while profit-making characteristics are those which describe how a corporation goes about actually generating revenue from whichever organisational form it has taken. 'Platform capitalism' thus describes a form of organisation which seeks to maximise the opportunities for profit by positioning themselves as intermediaries which bring people together and often provide tools for building products and services within that space, while 'surveillance capitalism' describes a mode of profit-making which seeks to track, analyse, and modify user behaviour so as to actually generate revenue. Rather than surveillance capitalism being an aspect of a subset of platform capitalism, we can understand that 'platform capitalism' refers to a particular form of organisation which seeks to maximise opportunities to make profit in a particular way, whereas 'surveillance capitalism' refers to particular mode of profit-making which is sometimes separate from and sometimes combined with platform capitalism.

3.1.2 | From Datafication to Control

So far we have seen what surveillance capitalism is and how it emerged, and have identified the rationality behind it. Now we move on to identify the dataveillance-based technology of power of surveillance capitalism and discuss how it operates through the computer mediation of big data so as to translate that rationality into reality by predicting behaviour and exerting control.

Building on the work of DeLanda on technology in warfare[31] and Deleuze on surveillance[32], Palmås calls this form of dataveillance, based on mass observation and experimentation in order to predict and influence user behaviour, 'panspectric' surveillance[33]. Unlike panoptic surveillance, which focuses on potentially observing an individual to control that individual[34], this kind of dataveillance focuses on observing the behaviour of a spectrum of millions of people at once so as to potentially influence the behaviour of any individual. Involving pre-emptive forms of control[35], panspectric dataveillance seeks to spot opportunities to intervene in future behaviour in order to direct it as desired. In 2008, Thrift predicted that we were moving towards a political economy of propensity in which the propensity of people to behave in certain ways in response to certain stimuli is exploited by corporations for profit[36]. In panspectric dataveillance, algorithmic regulation is employed to study users not as individuals, but as patterns and propensities of behaviour distilled from very large datasets[37] which can be used to predict individual user behaviour.

As we've seen, the corporations involved in surveillance capitalism rely fundamentally on algorithms. Google's early success as a search engine was built on the back of its famous PageRank algorithm, which ranks search results by importance based on the number and quality of links to a page[38]. And its subsequent vast profits from advertising have been generated using its AdSense and AdWords algorithms, the former of which is responsible for placing ads on Google's search results pages and the latter for placing ads on other websites. Facebook's News Feed algorithm, which ranks content for display every time a user visits the Facebook home page based both on what is popular and on what it determines that the user will want to see [39], is at its heart. Amazon's recommendation algorithm, which personalises the online store for each

[31] DeLanda, 1991
[32] Deleuze, 1992
[33] Palmås, 2011
[34] See Chapter 4.1
[35] Palmås, 2011, p.343
[36] Thrift, 2008
[37] Palmås, 2011, p.347
[38] Google, *Facts about Google and Competition*
[39] Oremus, 2016

customer based on their usage history, has been identified as a key factor in its success[40]. Algorithms are central in surveillance capitalism.

We will first discuss algorithmic regulation in this context from a governmentality point of view, before examining how this operates in practice by looking at how the individual is made hypervisible and behaviour is made predictable through surveillance and predictive analysis of big data, and will finally discuss the form of control used to direct user behaviour as desired.

Algorithmic Regulation and Governmentality

We saw in Chapter 1 that algorithms are tools of governance, of algorithmic regulation, in which they computationally generate knowledge from data in order to regulate behaviour in pursuit of some pre-specified goal. But, as we saw in Chapter 2, governance is concerned with the 'what' and the 'why' of government, whereas governmentality looks at the 'why' and the 'how'. A governmentality analysis of algorithmic regulation therefore allows us to go further and examine how algorithms are used in technologies of power for translating the rationality of surveillance capitalism into reality.

Antoinette Rouvroy has written extensively about the concept of 'algorithmic governmentality'. She identifies "*an unprecedented mode of government fuelled mostly with infra-personal, meaningless but quantifiable signals (raw data and metadata), addressing individuals through their 'profiles'*"[41]. In Rouvroy's view, "*the atunement of individuals' (informational or physical) environments and interactions according to their constantly evolving « profiles » … [opens] the way to pre-emptive action to secure commercial profit and forestall dangerous or sub-optimal behaviors*" [42]. Algorithmic governmentality involves a rationality founded on the automated collection, aggregation, and analysis of big data so as to predict and pre-emptively influence human behaviour[43]. The logic of

[40] Linden et al, 2003
[41] Rouvroy, 2015
[42] Rouvroy, 2015
[43] Rouvroy and Berns, 2013, p.X

accumulation of surveillance capitalism is one such rationality, and the technologies of power of algorithmic governmentality seek, as do all technologies of power in governmentality, to translate rationality into reality. This requires a government-type power interaction, and as in all government-type power interactions this means the creation of a contact point where a change in the behaviour of an individual is effected in order to produce a desired outcome.

For example, Bucher discusses how algorithms make people feel when they encounter them. Bucher looks at how and where people and algorithms meet[44], and describes some of the many ways that people consciously and subconsciously alter their behaviour in response to encountering the Facebook News Feed algorithm. This is where in governmentality the technologies of the self and of coercion meet – the contact point at which a government-type power interaction takes place. Some of those interviewed by Bucher routinely altered their behaviour in order to maximise the benefit that they found in the algorithm, while conversely some deliberately set out to confuse the algorithm and others even reported feeling angry when it made suggestions that they felt were inaccurate as they did not like the person that the algorithm 'thought' they were[45]. She notes that while none of the participants in her study have any knowledge of how Facebook's algorithm actually works, an example of algorithmic opacity and their invisible and unknowable nature, most of them had their own theories of varying degrees of complexity[46]. These users experience and respond to the algorithm in different ways, but what they share is that a change in their behaviour has been effected at the contact point of their regular encounter with an algorithm. The key to surveillance capitalism is in harnessing that potential for effecting a change in behaviour in order to direct it in the way desired.

[44] Bucher, 2017
[45] Bucher, 2017, pp.40-42
[46] Bucher, 2017, p.40

A governmentality-based analysis of how algorithms are combined with consumer surveillance in order to predict behaviour and exert control over the digital citizen in surveillance capitalism will identify this process as a technology of power that seeks to translate rationality of surveillance capitalism into reality. Rouvroy and Berns talk about the 'three stages' of algorithmic governmentality: first, the collection of big data in data warehouses; second, data processing and knowledge production; and third, action on behaviours[47]. They point out that these stages are interrelated and overlapping and are especially powerful because they mutually reinforce one another[48]. It is as a whole, therefore, that algorithmic governmentality can provide a particularly powerful mode of government, so it is as a whole that these three stages should be understood as the technology of power of surveillance capitalism. Rouvroy and Berns decline to connect algorithmic governmentality as a concept to any particular implementation[49], but these three stages will broadly speaking form the basis for our analysis. As such, the following will seek to provide an account of the technology of power of algorithmic governmentality as it operates in practice in surveillance capitalism, first through data collection, then through algorithmic analysis, and finally through the application of behavioural nudges based on this predictive analysis.

Surveillance and Datafication

This first stage of algorithmic governmentality involves the collection and storage of unfiltered big data[50]. The key this is obtaining as much data from as many sources as possible through surveillance and datafication. Indeed, it is only possible to perform the kind of predictive analysis involved in algorithmic governmentality with access to huge quantities of data. Datafication focuses algorithmic governmentality not on the real, physical person but on their datafied representations.

[47] Rouvroy and Berns, 2013, pp.VI-IX
[48] Rouvroy and Berns, 2013, p.X
[49] Rouvroy and Berns, 2013, p.IV
[50] Rouvroy and Berns, 2013, p.VI

There are several sources on which surveillance capitalism corporations rely. As well as their own surveillance operations, these corporations obtain significant amounts of data from data brokers. As a result, and while they provide data to a wide variety of companies involved in business of many kinds, fuelling a data economy that extends beyond surveillance capitalism, data brokers play an important role in surveillance capitalism. Companies like Axciom and Experian build comprehensive profiles of individuals, bringing together data from both online and offline sources, and provide a valuable source of personal and behavioural data to surveillance capitalism corporations. The exponentially-increasing processing power, as predicted by Moore's law[51], which can be applied to this data, as well as the ever-increasing capacity for data storage, allows for vast quantities of data to be collected for analysis. The databases that store this data are at the centre of an extensive surveillance apparatus, holding a wide range of personal information gathered through the monitoring of the everyday activities of consumers[52].

Much of this data, whether obtained directly by a surveillance capitalism corporation or from a data broker, comes from personal data that we voluntarily supply. But the bulk of it is behavioural data, obtained through surveillance. The gradual expansion of IoT devices feeding data back into databases has the potential to dramatically expand the quantity of this behavioural data available for reality mining. The spread of IoT devices involving cameras and microphones brings the possibility not just of an internet of *things* but also of an internet of *eyes* and *ears* feeding back into databases and potentially revealing a large amount of information directly about us as individuals beyond that revealed by data derived from our online interactions or from the sensor-laden smart devices that we use in our homes and carry with us everywhere.

[51] In 1965 Gordon Moore, the founder of Fairchild Semiconductor and Intel, predicted that due to advances in technology processing power would double every two years. This has proved to be an accurate prediction that still holds true (Pressman, 2017)
[52] Manzerolle and Smeltzer, 2011, p.324

The increasingly online nature of private, social, and economic life feeds directly into this data-gathering. Take, for example, the explosive growth in ownership of smartphones in the last decade. Google controls the development of the Android smartphone operating system, which is the most used smartphone operating system in the world, installed on 46% of all smartphones sold in the UK in 2016[53] and 88% sold worldwide[54], and which comes with Google apps – including its core search app – pre-installed as a condition of the licensing of the operating system to smartphone manufacturers. With nearly 9 of every 10 smartphones sold worldwide therefore coming with Google's software baked in – including all its data gathering tools and its apps for delivering targeted content to users – Google has unprecedented access to the most personal data about the daily lives of two billion people[55]. If you are a digital citizen who uses an Android smartphone then it's likely that not only does Google know your name, your age, your gender, where you live, your relationship status, and who you are friends with, but it also knows where you are, where you have been, what you search for, who you call and message, where you work, what you buy, what your emails say, what appointments you have, and a host of other highly personal information about you that can be fed into algorithms and used to predict and influence your future behaviour in order to extract the maximum possible profit from you. For these companies, computer mediation of personal and behavioural data means there is little that is unknown about the true digital citizen – as Siva Vaidhyanathan says, "*Google reads our minds, or at least Google simulates the reading of our minds*"[56].

Hypervisibility through Predictive Analytics

This is the second stage of algorithmic governmentality. Zuboff calls this informating, while Rouvroy and Berns call it 'knowledge production'[57], and it's commonly known as 'reality mining'[58]. These are substantively the same thing,

[53] Statista, 2016
[54] Forrest, 2016
[55] Popper, 2017
[56] Vaidhyanathan and Bulock, 2014
[57] Rouvroy and Berns, 2013, p.VII
[58] Pentland, 2009, p.76; Zuboff, 2015, p.84;

and involve subjecting the data gathered in the first stage to algorithmic analysis in order to provide insights into users from which predictions can be made. Yeung identifies this as the 'information gathering' component of algorithmic regulation[59], in this case taking a pre-emptive form by which future behaviour is predicted so that it can be intervened upon[60].

While this kind of analysis can only provide insight into correlations, the predictive power of algorithms should not be underestimated. A 2010 study of mobile phone location data found that the movement behaviour of users could be predicted with 93% accuracy[61]. And, as discussed previously, highly personal information about an individual can be determined through predictive analysis of impersonal behavioural data, such as that relating to Facebook Likes. Ayres, who calls this 'Super Crunching'[62], says that algorithmic analysis "*will predict what you will want and what you will do*"[63], meaning that corporations may be able to more accurately predict your behaviour than you ever could yourself[64]. In Pentland's view, reality mining provides the capacity to collect and analyse data about people with a previously inconceivable breadth and depth[65], giving us a "*a God's eye view of ourselves*"[66]. As companies gather ever more data and as technology exponentially advances, algorithmic predictions will become ever more accurate and detailed[67].

The individual is made visible and knowable by surveillance, datafication, and the analytical power of the invisible and unknowable algorithm. When it comes to the corporations to which we are willingly providing vast quantities of the most personal data imaginable there is and can be no such thing as true privacy[68]. Surveillance capitalism requires us to be visible, and through mass

[59] Yeung, 2017b, p.7
[60] Yeung, 2017b, p.8
[61] Song et al, 2010, p.1018
[62] Ayres, 2008
[63] Ayres, 2008, p.44
[64] Ayres, 2008, p.33
[65] Pentland, 2009, p.77
[66] Pentland, 2009, p.80
[67] Pentland, 2009, p.76
[68] For a further discussion of privacy in surveillance capitalism see Chapter 6.1

participation in the online world and the datafication and analysis of our lives the digital citizen is not just visible but *hypervisible* to the companies engaged in this new form of capitalism.

Hypervisibility in the Internet of Things

For the most part this hypervisibility has until recently been limited to the analysis of data produced as we move through the digital world. However, Rouvroy and Berns note that software can now recognise and datafy emotions, facial movements, and skin tones[69]. For example, in 2017 Amazon announced its 'Echo Look' device, which would take full-body photos of customers and will analyse them in order to help users dress and give fashion advice[70]. Vincent highlights what kinds of insight these kinds of devices could potentially provide to corporations:

> *"Think about it. If you pass a stranger in the street, how much information do you get with a second's glance? You can probably make some decent estimates about their height, weight, age, race, and gender. If they were far enough along in pregnancy, you'd know. And you could take a stab at other, more contentious questions, like: are they rich or poor? Friendly or closed-off? Are they having a good day? If it takes a second for you to answer these questions, then Amazon's AI could take a stab at it as well. And, given enough data, it can offer far, far more accurate answers."*[71]

In the IoT the digital citizen becomes hypervisible both in a figurative and in a literal sense, potentially and more readily revealing a wealth of information about their immediate emotional state, health, or other aspects of life. Beyond microphones and cameras, the internet of things promises to bring monitoring, tracking, and predictive analysis into many areas of everyday life, creating a

[69] Rouvroy and Berns, 2013, p.VI
[70] Palladino, 2017
[71] Vincent, 2017

physical architecture for surveillance capitalism and extending its reach beyond the digital and into the real world and offline public space.

Control through Hypernudging

This forms the third and final stage of algorithmic governmentality, and involves using the information produced by the algorithmic analysis of earlier stages to create ways to influence behaviour. Yeung calls this the 'enforcement and behaviour modification' component of algorithmic regulation[72]. She shows how dataveillance in surveillance capitalism uses prediction based on computer mediation of past group and individual behaviour to produce behavioural nudges in order to exert a form of control over the individual in the hope of effecting a desired outcome[73]. Building on the fact that much human decision-making takes place subconsciously and unreflectively rather than through active deliberation[74], and taking advantage of known vulnerabilities in decision-making, including the use of heuristics and the resulting prevalence of cognitive biases, the concept of nudges for behaviour modification was first put forward by Thaler and Sunstein. They describe them as "*any aspect of choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives*"[75]. While nudging as a form of behaviour modification is not unique to dataveillance, the confluence of several factors that are unique to big data mean that nudging in this context can be particularly effective.

Yeung calls this form of control, a highly amplified form of nudging unique to big data, 'hypernudge'[76]. She argues that there are two key factors that distinguish hypernudges in the digital world from nudges in the real world[77] – the fact that they can be highly personalised, and the fact that they can altered dynamically in real time in response to user behaviour, neither of which are true of real-

[72] Yeung, 2017b, p.7
[73] Yeung, 2017a
[74] Yeung, 2017a, p.120; Kahneman, 2012
[75] Thaler and Sunstein, 2008, p.8
[76] Yeung, 2017a
[77] Yeung, 2017a, p.122

world nudges. As Yeung puts it, with the personalised, dynamic, and responsive nature of digital spaces, "*these nudges channel user choices in directions preferred by the choice architect through processes that are subtle, unobtrusive, yet extraordinarily powerful*"[78].

Yeung identifies two forms of decision-making associated with dataveillance – 'automated decision-making processes', which involve a machine making a decision based on data analysis, and 'digital decision-making processes', which target an individual based on data analysis in order to lead them to make a desired decision[79]. While automated decision-making processes do have implications for the individual in society, the latter, which seek to direct an individual's decision-making in the way deemed optimal by the underlying algorithm by offering suggestions intended to prompt the individual into making the desired decision[80], is our focus in this instance. Yeung provides the example of a Google search result page to demonstrate how this works in practice:

> *"In the Google search engine, for example, the most prominently displayed sites are 'paid for' sponsored listings (thus enabling firms to pay for search engine salience), followed by weblinks ranked in order of Google's algorithmically determined relevance. Although theoretically free to review all the potentially relevant pages (from the hundreds of thousands ranked), in practice each individual searcher is likely to visit only those on the first page or two … Hence the user's click-through behaviour is subject to the 'priming' effect, brought about by the algorithmic configuration of her informational choice architecture seeking to 'nudge' her click-through behaviour in directions favoured by the choice architect. For Google, this entails driving web traffic in directions that*

[78] Yeung, 2017a, p.119
[79] Yeung, 2017a, p.121
[80] Yeung, 2017a, p.121

> *promote greater use of Google applications (thereby increasing the value of Google's sponsored advertising space)."*[81]

This kind of control is prevalent both on the web and in the mobile apps produced by companies such as Google and Facebook. Links and associated information are often determined algorithmically in order to induce a desired behaviour in the user. Indeed, as Rouvroy and Berns point out, "*the aim is of course precisely not so much to tailor the offer to individuals' spontaneous desires (assuming such a thing exists), as to adapt those desires to the offer by tailoring sales strategies (the way of presenting the product, of pricing it, etc.) to each person's profile*"[82]. The way in which nudges operate in the digital to achieve this is vastly more sophisticated than in the offline world.

Algorithms can continuously update suggestions on the fly to account for changes in behaviour or to offer new suggestions in repeated attempts to induce the desired behaviour should those previously proffered be ignored by the user. As a result, they can dynamically provide more relevant and, in theory, more effective nudges based on changing circumstances and tailored both to take into account changing trends in the behaviour and responses of users generally and to reflect the variable and unique behaviour of the targeted individual specifically[83]. As both a response and a lack of response from a user can be taken into account in future attempts to provide more effective nudges, there is, in effect, no such thing as failure. Every nudge, whether acted upon or not, provides an opportunity to learn more about an individual user's behaviour and to feed this into models that predict the behaviour of people more generally so as to more effectively influence that behaviour. Rouvroy and Berns put it like this:

> *"Algorithmic governmentality, with its perfect adaptation in 'real time', its 'virality', (the more it is used, the more the* algorithmic

[81] Yeung, 2017a, p.121
[82] Rouvroy and Berns, 2013, p.XIII
[83] Yeung, 2017a, p.122

> *system is refined and improves, since all interaction between the system and the world translates into a recording of digitized data, correlative enrichment of the 'statistical base', and improvement of the algorithms' performance) and its plasticity, renders the very notion of 'misfire' meaningless; in other words, a misfire cannot 'jeopardize' the system, it is immediately re-ingested to further refine behavioural models or profiles"*[84]

As previously noted, data models produced by analysis of behavioural surplus will only show correlations in consumer behaviour. This may lead to an inaccurate picture being produced[85], and, as Rouvroy points out, it is important to remain wary of the sufficiency of correlations[86]. Key to refining data models in order to more accurately predict behaviour is taking advantage of the ability to learn from failure by deliberately experimenting with different nudges, both in terms of the form of nudges themselves and in terms of the contexts in which they are provided, which allows analysis to move beyond identifying correlation to potentially identifying causation[87]. Google as of 2014 ran about 10,000 experiments a year, with around 1,000 running at any given time[88]. In 2008 these experiments resulted in 450-500 changes in the system, tweaking everything from the background colour of ads and the spacing between ads and search results, to the underlying ranking algorithm[89]. When you use Google you are unwittingly participating in dozens of experiments at once. Continual experimentation like this – "*pretty easy to do on the web*", according to Varian[90] – would be impossible with nudges in the offline world. A speed hump, an example of an offline nudge, cannot be continually repositioned in order to determine the best location to most effectively reduce a particular driver's speed on a particular street, but in digital space this kind of experimentation is commonplace. Businesses have, of course, always experimented in one way or

[84] Rouvroy and Berns, 2013, p.XI
[85] Hofacker et al, 2016, p.94
[86] Rouvroy and Berns, 2013, p.VIII
[87] Varian, 2014
[88] Varian, 2014
[89] Varian, 2010, p.5
[90] Varian, 2014

another, but the availability of computer mediation makes these experiments cheaper and more flexible than ever before[91]. Google's experiments are successful enough that they have been made available to advertisers, allowing them to experiment with different factors in order to find the optimal settings for their ads[92]. In the offline world nudges simply do not have this capacity to learn as they go and can be neither anywhere near as dynamic nor anywhere near as personalised. Dataveillance therefore uses our personal and behavioural data to provide a highly individualised, dynamic, and reactive form of control that does not – and *could* not – exist in the offline world. It is this difference between offline and digital nudges that leads Yeung to describe this form of control as 'hypernudge'[93].

Remember that in our governmentality analysis government is a power interaction located at the contact point where the technologies of the self (our self-management, and the techniques through which we manage our own behaviour) and technologies of coercion (the techniques through which others compel us to act in certain ways) combine to govern conduct – the *conduct of conduct*. It is primarily through combining big data surveillance, analytical techniques, and these algorithmically produced, highly dynamic, highly personalised hypernudges as a technology of power in algorithmic governmentality that corporations seek to create this contact point and effect a change in behaviour so as to translate the underlying rationality – the logic of accumulation of surveillance capitalism – into reality.

We can now understand how algorithmic governmentality operates in surveillance capitalism, and can identify its rationality and its technology of power. Next we will examine what this means for the digital citizen in terms of their role within surveillance capitalism and how the practices of surveillance capitalism appropriate the sovereignty of the individual – the central concept of neo-liberal theory – for corporate ends.

[91] Varian, 2010, p.6
[92] Varian, 2014
[93] Yeung, 2017a, p.122

3.2 | The Digital Citizen in Surveillance Capitalism

Now that we know what surveillance capitalism is (in terms of its rationality) and how it operates (in terms of its technology of power) we can discuss what it means for the digital citizen. In his analysis of modern western society's shift from being a *disciplinary* society, described by Foucault[94], to a *control* society, operating with computers, Deleuze argues that the individual is no longer the smallest unit in that society[95]. He observes that 'individual' means 'indivisible', but that consumer surveillance turns the individual into a 'dividual'[96] – a divisible assemblage of the component parts of the individual. As Williams puts it, the dividual is "*a physically embodied human subject that is endlessly divisible and reducible to data representations via the modern technologies of control, like computer-based systems*"[97].

In a control society the point isn't to make real bodies docile, but to mould people as consumers through their data bodies[98]. In surveillance capitalism, the goal is not to control people as physical entities, but to use datafied representations of them to predict and influence their behaviour as consumer-citizens in all areas of life. Datafication in this context involves abstracting human bodies and behaviour from the real world into data points which can then be assembled into profiles – what Heggarty and Ericson call 'data doubles', composed of pure information[99] – and analysed and targeted for intervention. This involves building profiles of individuals and models of behaviours without ever involving the individual, and without asking them to describe what or who they are, so these data doubles can only ever be representations of our datafied component parts as constructed by others[100]. Yet our data double operates as a shadow self that stands in for our physical self and allows us to be subjected to predictive analysis and therefore the control of algorithmic governmentality.

[94] Foucault, 1991
[95] Deleuze, 1992, p.7
[96] Deleuze, 1992, p.7
[97] Williams, 2005
[98] Galič et al, 2017, p.20
[99] Heggarty and Ericson, 2000, p.613
[100] Rouvroy and Berns, 2013, p.X

Foucault argues that disciplinary societies engage in individuation[101], where government is focused on the individual, measuring them against an idealised norm. Similarly, we could say that the reduction of the individual to the dividual is a process of *dividuation*, where the datafied component parts of the dividual are variously analysed and held to different norms. Hintz et al echo Isin and Ruppert's description of the digital subject as a composite[102] of multiple identifications, affiliations, and associations to describe an ongoing fragmentation and a loss of classic reference points for citizenship[103]. Instead the digital citizen is cast anew. Foucault wrote of power which is capillary, and which affects "*the grain of individuals, touches their bodies and inserts itself into their actions and attitudes, their discourses, learning processes and everyday lives*"[104]. Through algorithmic governmentality in surveillance capitalism the digital citizen is remade according to a new rationality.

In this the digital citizen becomes splintered, and rather than being the well-informed active consumer-citizen freely engaged in perpetual choice-making in pursuit of their own self-interest of the neo-liberal ideal, they are reduced to their datafied constituent parts – name, age, gender, location, likes, dislikes, friends, relatives, etc. – and take on a new role. We will first examine how they become simultaneously a *producer* and a *consumer* of content – what has been called a 'prosumer' – but therefore also a *producer* of behavioural surplus through both production and consumption, will introduce new terms to account for this new role, will see how this facilitates the commodification of the digital citizen, and will attempt to determine whether or not the digital citizen in this role is exploited in surveillance capitalism. We will then discuss how in taking on this multi-faceted role, and through the asymmetry of information between the visible, knowable computer-mediated digital citizen and the corporation with its access to the most personal information about us and its invisible, unknowable algorithms, the sovereignty of the individual, the key concept in

[101] Foucault, 1991, p.193; Galič et al, 2017, p.17
[102] Isin and Ruppert, 2012, p.12
[103] Hintz et al, 2017, p.733
[104] Foucault, 1980, p.39

neo-liberalism, becomes appropriated and turned against the digital citizen for profit.

3.2.1 | The Role of the Digital Citizen

Various writers, most ambitiously George Ritzer, have written about a new role for the digital citizen as a producer-consumer, or 'prosumer'[105]. For Ritzer, prosumption involves an interrelationship between production and consumption in which it is difficult, if not impossible, to clearly distinguish one from the other[106]. Ritzer recognises that production and consumption have always been linked, and that capitalism has always involved a dual role for the individual – a prosumer acting as both a producer and a consumer[107]. In his view, while the individual has always played this dual role, over successive stages of capitalism the relationship between the two components of the prosumer has changed[108]. As a result, he argues, production capitalism was 'singly' exploitative as it involved exploitation of the prosumer primarily as a producer, and consumer capitalism was 'doubly' exploitative as it involved exploitation of the prosumer as both a producer and a consumer but in different ways and in different spaces[109], but in the digital world the exploitation of the prosumer as a consumer and as a producer now occur in the same place and at the same time, taking exploitation to a new form and an unprecedented level[110]. He argues that as a result of this temporal-spatial unity of exploitation, capitalism in the digital is "*synergistically doubly exploitative*"[111]. Ritzer further argues that the emergence of this new form and level of exploitation of the prosumer signals the emergence of a new form of capitalism, which he terms 'prosumer capitalism', centred on this simultaneous exploitation of the prosumer as a producer and a consumer[112]. This claim is vigorously and

[105] See, e.g., Ritzer, 2015; see also Toffler, 1980
[106] Ritzer, 2015, pp.413-414
[107] Ritzer, 2015, p.417
[108] Ritzer, 2015
[109] Ritzer, 2015, p.425
[110] Ritzer, 2015, p.426
[111] Ritzer, 2015, p.425
[112] Ritzer, 2015

reasonably contested by Zwick on a number of grounds, including that Ritzer goes too far in elevating prosumption to the level of a new form of capitalism and in the extent to which he claims that prosumers are exploited and that he doesn't go far enough in considering the degree to which marketing turns consumers into mass producers[113].

While Ritzer's argument is persuasive in places, it should also be noted that his analysis claiming a new form of capitalism looks largely at the role of the individual, focusing on one aspect of the political economy at the expense of others and arguing from this narrow focus that a change in the whole has occurred without demonstrating a significant shift in other aspects of that whole (for example changes in the underlying model of accumulation such as those which delineate industrial, financial, and surveillance capitalism). More significantly, his analysis also fails to account for the role of behavioural surplus in surveillance capitalism – remember that it is through the use of our behavioural data, not through the use of our content as Ritzer's analysis would have it, that corporations such as Google and Facebook generate most of their profits (although there is money in content, it can often be accessed for free to draw users in since the behavioural surplus that they will produce in consuming that content is potentially far more profitable). In our analysis, therefore, it would be more accurate to discuss the behavioural surplus generated by the prosumer acting simultaneously as a producer and a consumer of content as being an important component part of the new form of capitalism known as surveillance capitalism, not as heralding a new form of capitalism in and of itself.

In surveillance capitalism, the digital citizen is the source of the raw material – behavioural surplus – from which the profits of corporations are ultimately derived[114]. The following will propose the concept of the 'produsumer' in order to account for this new role, and will seek to determine whether the digital citizen as a producer of behavioural surplus is exploited in surveillance

[113] Zwick, 2015
[114] Zuboff, 2016, p.6

capitalism. Whether this is the case depends to a large extent on whether or not they are producing valuable work without reward. So in order to determine the answer to this question we will first identify production of behavioural surplus as being a form of work and will determine what kind of work this is, before the describing the commodification of the surplus produced through this work and finally addressing the question of exploitation.

Production

To show how generation of behavioural surplus should be considered to be work we can look to Fuchs's demonstration of how production of content – whether that be, for example, websites that are indexed by Google search or posts and photos on Facebook that draw in other users – should be considered to be work[115]. Content is vitally important to many online services, and Fuchs uses the question of what would happen if this was withdrawn to demonstrate that its production is labour:

> *"The number of users would drop, advertisers would stop investments because no objects for their advertising messages and therefore no potential customers for their products could be found, the profits of Google would drop, and the company would go bankrupt. If such activities were carried out on a large scale, a new economy crisis would arise"*[116]

As production of content generates surplus value for Google, it should be recognised to be work. Fuchs's argument echoes that made by Lazzarato, of the Italian autonomist school of thought, about immaterial labour[117]. This states that in an information society, dominated by ICT, the production of the informational and cultural aspect of an immaterial commodity should itself be considered to be work as it is that informational and cultural content that

[115] Fuchs, 2011
[116] Fuchs, 2011
[117] Lazzarato, 1996

provides the commodity's value. A similar argument has also been put forward by Terranova, following from Lazzarato[118].

So as the production of content is work, what about the production of behavioural surplus? Clearly, and even more so than the production of content, the production of behavioural data creates surplus value for Google – behavioural surplus is, after all, the raw material from which they ultimately derive around 90% of their profit[119]. And if behavioural surplus was withdrawn then Google's business model would collapse. So, following Fuchs, the production of behavioural surplus should be considered to be work just as the production of content can be considered to be work[120]. And if we follow Lazzarato and Terranova, the production of behavioural surplus creates the informational value of the principal commodity of surveillance capitalism – the data profiles bought and sold on the advertising market – and so should be considered to be work. We can therefore recognise behavioural surplus, the raw material of surveillance capitalism without which the vast profits drawn from dataveillance would be impossible, as being generated through the work of the digital citizen. As we can consider the generation of behavioural surplus to be work, we can consider first what kind of work this is and then the extent to which this work is exploited.

As behavioural data is generated by both our production and our consumption of content it could be said that through dataveillance both production and consumption become productive[121]. It is in this sense, more than any other, that we take on a new role in surveillance capitalism – through both production and consumption of content we become a productive source of raw material, often without being aware that this is happening[122]. We could call this role the *produsumer* to distinguish from the prosumer of Ritzer's and others' analyses, in which individuals act as producers and consumers of content as a role in and of

[118] Terranova, 2000
[119] Rosenberg, 2016
[120] Fuchs, 2011, p.10
[121] Andrejevic, 2012, p.84; see also Andrejevic, 2011
[122] Turow, 2012.

itself rather than as producers of behavioural surplus through both production and consumption of content, and in doing so emphasise the productive nature of both production and consumption.

Goss argues that the adoption of the practices of what we can recognise as surveillance capitalism is an attempt to bring consumption under the control of production[123]. Compare this with what Kotz describes as neo-liberal capitalism's domination of labour by capital[124]. Kotz notes that every form of capitalism must stabilise the relationship between labour and capital in some way[125]. Zuboff argues that surveillance capitalism involves a parasitic form of profit[126], and in this the relationship between labour and capital is one in which not just productive labour is dominated by capital, as in neo-liberalism, but in which productive labour is united with what we could call *consumptive labour* as a new form of production and together they are brought within the dominion of capital.

Consumptive labour can be distinguished from productive labour in surveillance capitalism in that productive labour in this context involves producing behavioural surplus through the production of content and consumptive labour involves producing behavioural surplus through the consumption of content. And consumptive labour is perhaps the primary way by which the individual produces behavioural surplus. Fuchs, however, in his Marxian analysis considers all production of behavioural data to be productive labour in the same vein as production of content, with no distinction as to the origin of the surplus, and therefore prosumption[127]. But this cannot be correct. Marx wrote that at the "*end of every labour process, a result emerges which had already been conceived by the worker at the beginning, hence already existed ideally*"[128]. As Fuchs himself says, this means that "*All human labor requires*

[123] Goss, 1995, p.172; and see Chapter 3.2.2, below, on the appropriation of consumer sovereignty in surveillance capitalism
[124] Kotz, 2015, p.43
[125] Kotz, 2015, p.43
[126] Zuboff, 2016
[127] Fuchs, 2011, p.10
[128] Marx, 1990, p.284

mental planning and anticipation of the result"[129]. Thus productive labour involves some form of intention to produce, or anticipation of producing, what is produced. Or, as Jeon puts it, productive labour "*presupposes knowledge of the goal of the labor (i.e., what to produce) and the techniques to realize the goal (i.e., how to produce)* "[130]. Yet in the production of behavioural surplus through consumption this is not always, or perhaps even often, the case. It is unlikely indeed that many people are using Facebook with the goal of providing them with behavioural data – many, if not most, are at least some of the time using Facebook with the intention not of producing anything for anyone but of consuming content. They may not even be aware that through consumption they are producing anything at all. So production of behavioural surplus through consumption cannot be productive labour, and the work of the digital citizen performed through consumption cannot be located within a traditional Marxian analysis. Marx's concept of labour, upon which Fuchs builds his analysis, cannot include the production of behavioural surplus through consumption and therefore cannot adequately explain the role of the individual in surveillance capitalism. Consumptive labour therefore takes us beyond Fuchs's analysis, and beyond Marx.

However, uploading a photo to Facebook or Instagram, for example, *can* be considered to be productive labour as the user knows that the site will store data about it, will associate it with their profile, will show it to others, and will track it how it is interacted with. Indeed, these will often be the reasons for uploading the photo in the first place. As such, the user is not just aware that in uploading the photo they will produce behavioural surplus, although they may not think of it in those terms, but is often uploading it with the intention that this will happen. So while most work in surveillance capitalism is consumptive, some is productive. And while productive labour and consumptive labour can and should be distinguished, it is in the union of these two forms of labour, both of which are performed by the digital citizen in surveillance capitalism, often simultaneously, that we find the work of the produsumer.

[129] Fuchs, 2017, p.68
[130] Jeon, 2011, p.199

And consumptive labour should also be distinguished from Marx's concept of productive consumption. Marx argued that as things are productively consumed in order to produce other things, consumption and production are correlates and come hand-in-hand, giving the example of a man consuming food to produce body[131]. But in surveillance capitalism this does not hold. Behavioural surplus is produced as a by-product of consumption, rather than consumption being a precursor to production as in Marx's analysis. Consumptive labour therefore involves production as a side-effect of consumption, rather than consumption in order to produce. Hence consumptive labour (production through consumption) rather than productive consumption (consumption for production). In any case, both productive and consumptive labour come together to form a new kind of production in surveillance capitalism – *produsumption* – undertaken by the digital citizen as a produsumer. In produsumption both productive labour and consumptive labour are sources of raw material to be brought within the control of capital through algorithmic governmentality.

As well as a new cycle of accumulation that moves beyond Marx's analysis of previous forms of capitalism, surveillance capitalism therefore also involves a new form of labour that also moves beyond Marx's analysis of previous forms of capitalism. And it is in the combination of this new form of labour (consumptive labour) with existing forms of labour (productive labour) that we find the new role for the digital citizen – the produsumer. Now that we can identify produsumption as work, and can identify what form this work takes, we can move on to see how the produsumer's work allows the digital citizen as a produsumer to be commodified, before moving on to determine whether this facilitates their exploitation.

[131] Marx, 1859, p.196

Commodification

As digital citizens we become commodities in surveillance capitalism[132]. The behavioural surplus generated by the labour of the produsumer is its raw material, and is subject to predictive algorithmic analysis in order to produce a commodity to be sold on the advertising market for profit. The transformation of the digital citizen into a series of data points allows a user profile to substitute for the real-world individual[133], and thus the digital citizen's commodification. In this we become representations of our physical selves; data doubles of produsumers that can be computer-mediated and so made visible, knowable, and saleable.

Peterson describes how social media transforms users into commodities to be sold on the market[134] and while, as Bauman observes[135], there has long been an element of consumer-as-commodity in consumer capitalism[136], in surveillance capitalism this takes on a different nature. In consumer capitalism, the individual may often have to commodify and sell themselves in order to 'get ahead' (as a prospective employee sending out CVs to employers, for example). But, as we saw in Chapter 2[137], neo-liberal digital citizenship involves self-commodification and self-promotion through online identity performance, often to gain social approval – curating Facebook profiles to present the self in the desired way, or posting carefully-posed selfies in the hope of receiving likes, for example. As we've seen, in this it is not just the individual selling themselves to friends or potential employers according to their own desires, but the surveillance capitalism corporation shaping the process of identity performance and thus self-commodification according to its desires[138]. In surveillance capitalism this self-commodified individual is combined with the behavioural surplus generated through their work as a produsumer, packaged as a data

[132] See, e.g., Brown, 2010; Fuchs, 2011; Solon, 2011; Felten, 2014
[133] Bauman, 2007, p.14
[134] Peterson, 2008
[135] Bauman, 2007, p.6
[136] Bauman, 2007, p.12
[137] Chapter 2.4.3
[138] van Dijck, 2013, p.212

profile, and sold as a commodity to other corporations for profit. While television and radio advertising has long relied on the commodification of consumers, in the past this took the form of commodifying the audience as a whole, or as segments of the whole[139]. In surveillance capitalism, and while of course the digital citizen remains the audience for advertisers, this becomes individualised, based on the user's commodified self and their behavioural profile. Rather than segments of consumers as a group being sold as commodities to advertisers, the digital citizen as an individual is datafied and sold as a commodity to advertisers. This is perhaps the next logical step: first the neo-liberal digital citizen turns themselves into a commodity to meet the demands of a consumer society whose norms are often dictated by corporations[140]; next the self-commodified digital citizen is made hypervisible and knowable through computer mediation; and then they are sold as a commodity for profit and subjected to new forms of control. This takes us beyond the analysis of Bauman and the consumer society into something new – a surveillance capitalism society, in which the corporation monetises our life for their profit.

In this, data profiles stand-in and speak for the real individual[141], and much of this occurs without the knowledge of the digital citizen, who is often neither aware that their data doubles are being bought and sold, nor aware of who they are being bought and sold by. Through computer mediation in the logic of surveillance capitalism the digital citizen is reimagined as a disembodied data double with an exchange value like any other commodity[142]. The process of datafying the digital citizen based on their work as a produsumer thus not only renders them amenable to the control of algorithmic governmentality, but also allows them to be sold on the advertising market for profit. It is this commodification – turning the composite of our datafied selves and the behavioural surplus that we generate into a commodity to be bought and sold on the advertising market – that makes the work of the produsumer truly

[139] Smythe, 2001
[140] Bauman, 2007, p.6
[141] Manzerolle and Smeltzer, 2011, p.326
[142] Manzerolle and Smeltzer, 2011, p.327

valuable in surveillance capitalism. So it is on the basis of this commodification of the produsumer – which builds on the self-commodification performed by the digital citizen as a neo-liberal subject – that we can attempt to determine whether or not the digital citizen is exploited as a produsumer.

Exploitation

In 2000, Terranova looked at the free labour performed by chat room moderators in exchange for services and argued that "*free labour is the moment where this knowledgeable consumption of culture is translated into productive activities that are pleasurably embraced and at the same time often shamelessly exploited*"[143]. In a similar way, the digital citizen engaging with the online world as a produsumer generates vast quantities of behavioural data through free labour in their embrace of the digital, and the surplus produced by this labour is exploited through commodification in order to extract profit without their financial gain[144].

Our generation of behavioural surplus through produsumption – whether in the form of productive or consumptive labour – and the vast profits that are derived from it through the commodification of the produsumer both occur in such a way that many people may be entirely oblivious to the fact that it is happening, calling into question whether the average digital citizen is aware of the true value of what they're producing. While it could, therefore, be argued that produsumers are to some extent exploited in that the surplus generated by their work is collected, commodified, and sold by Google, Facebook, et al. for profit without recompense and potentially without their knowledge, we should be mindful of Zwick's issues with Ritzer's analysis of the prosumer in terms of the degree to which exploitation occurs, which he also levels at Fuchs's claims of exploitation and which arguably could also apply to Terranova. While Zwick agrees that "*exploitation of the productive forces of the individual remains at the*

[143] Terranova, 2000, p.37; see also, e,g, Petersen, 2008 and Halvais, 2009
[144] See Fuchs, 2011

center"[145], and accepts that "*proliferation of prosumer work, and correspondingly its exploitation, has been helped along dramatically by the emergence of collaborative media, such as Web 2.0*"[146], that the profits and value of internet companies "*can be explained by the accumulated labor value of millions of unpaid producers*"[147], and that the "*variety of the work done by its users could never be accomplished by Facebook itself*"[148], he makes the point that clearly the users of these services receive something in return or else they wouldn't keep using them. The same could be said to an extent with the produsumer. Where the prosumer receives in return interaction both with other prosumers and with consumers – say, a band who uploads their music to YouTube and can therefore gain interaction both with other prosumers (other bands) and consumers (the audience) – the produsumer receives in return interaction with other produsumers and/or the use of an online service that they may enjoy or find useful, enjoyable, or interesting.

However, as Andrejevic argues, exploitation isn't just about a loss of monetary value, but also a loss of control over productive and creative activity[149]. And if, as in Lazzarato's analysis, it is the informational and cultural content of an immaterial commodity that gives it value, then loss of control of the surplus stemming from that informational and cultural content, which is generated through produsumption, can also be exploitation. So it would perhaps be accurate to conclude that in surveillance capitalism the digital citizen takes on a new role as a produsumer and is exploited in that they lose control of the surplus of their work and it is instead commodified, allowing the digital citizen to be sold by for profit without *sufficient* recompense for their true value – a value that these companies have a vested interest in the digital citizen neither knowing nor realising.

[145] Zwick, 2015, p.491
[146] Zwick, 2015, p.491
[147] Zwick, 2015, p.491
[148] Zwick, 2015, p.491
[149] Andrejevic, 2011, p.284

This process of datafication, commodification, and exploitation of the digital citizen is just one half of how surveillance capitalism remakes the relationship between corporations and the digital citizen. The other, which we come to now, lies in the way that this process creates informational asymmetries between the corporation and the individual which result in the appropriation of the sovereignty of the neo-liberal digital citizen and facilitate their control by corporations.

3.2.2 | The Appropriation of Consumer Sovereignty

One of the key reasons put forward in neo-liberal theory for why the free market should be unregulated and prioritised is that it mediates transactions between sovereign consumers[150]. The concept of the sovereign consumer leads to the active consumer-citizen, expected to freely engage in perpetual choice-making in pursuit of their own self-interest, as described in Chapter 2. Manzerolle and Smeltzer argue that a principal aspect of online consumer surveillance is the articulation of consumer sovereignty for two purposes in pursuit of commercial interests[151] – to better tune production and to help create consumer wants and needs. In their view, the sovereignty of the consumer is invoked – implicitly or explicitly – in order to justify surveillance of the consumer, often in the language of providing choice or of giving the consumer what they want. For them, it is important to note that this articulation of consumer sovereignty is the result of "*the ideological fusion of neoliberal capitalism and information society utopianism; a belief that with additional information and the progressive powers of ICTs society will function more smoothly, equitably, and democratically*"[152]. This remains the case in surveillance capitalism, but the pervasive surveillance of online behaviour and subsequent predictive algorithmic analysis also creates informational asymmetries between the corporation engaged in these practices and the digital consumer-citizen engaged in the process of perpetual choice-making in the online environment.

[150] Fellner and Spash, 2014
[151] Manzerolle and Smeltzer, 2011
[152] Manzerolle and Smeltzer, 2011, p.325

Such informational asymmetries, in which the individual is hypervisible and the corporation shrouds its activities in algorithmic opacity, allow control to be extended over the digital citizen through hypernudging and their behaviour to be influenced as desired by the corporation. And these informational asymmetries mean that it is not only the digital citizen that is commodified in surveillance capitalism. Advertisers gain access to the knowledge required to influence the exercise of the social and economic agency of the consumer-citizen as the sovereign actor of neo-liberalism, so that sovereignty itself also becomes commodified and sold for profit. The three stages of algorithmic governmentality as employed in surveillance capitalism therefore mean that corporations move beyond merely *articulating*, or invoking, consumer sovereignty in order to justify their practices, although this articulation still occurs, to now also *appropriating* that sovereignty in order to facilitate and further those practices for corporate ends.

This appropriation involves presenting the expansion of the online world as being an expansion in consumer freedom and choice, while in reality the asymmetries of information that exist between the digital citizen and the corporation have made the former more amendable to control by the latter than ever before. While in neo-liberal theory a flow of information to and from the consumer is essential for the functioning of the market[153], surveillance capitalism requires a flow of information from the individual to the corporation (through the gathering and analysis of behavioural data), and from corporation to corporation (through the sale of user profiles on the advertising market), but not from the corporation to the individual. This manifests both in algorithmic opacity, as discussed previously[154], and in a general lack of information about corporations and their business practices. As a result, while corporations may know the most intimate details about an individual's life and may know how to most effectively influence their behaviour[155], the individual may know very little indeed about the corporation or about how their data is being used. This is often

[153] Manzerolle and Smeltzer, 2011, p.325
[154] See 4.1.2
[155] Manzerolle and Smeltzer, 2011, p.324

justified on the basis that the corporation needs to 'listen' to the consumer in order to provide them with their desired product or service[156], and while it may seem that this is in fact an expression of consumer sovereignty – in that the consumer can 'instruct' the corporation on how best to meet their desires – the informational asymmetry created by this unidirectional flow of information in reality undermines the power and therefore the sovereignty of the consumer.

As we have seen, computer mediation of the vast quantities of data gathered about an individual consumer renders them visible and knowable to an unprecedented degree and allows corporations to predict and influence their future behaviour. As well as a flow of information, therefore, surveillance capitalism involves a flow of *knowledge*, therefore a flow of *power*, and therefore a flow of *sovereignty*, from the consumer to the corporation. Hintz et al observe that we are "*confronted with the emergence of a new power dynamic; one that is premised on an order of 'haves' and 'have nots' between those who provide personal data (digital citizens) and those who own, trade, and control it (typically, large Internet companies and the state)*"[157]. Far from the flows of information to and from the consumer that are essential for the functioning of the market in neo-liberal theory, the asymmetry of information inherent to surveillance capitalism entrenches the asymmetry of power between the consumer and the corporation and facilitates the appropriation of the sovereignty of the consumer.

Information is of use primarily in generating knowledge, and when we talk about asymmetry of information we should recognise that what we are really talking about is an asymmetry of *potential knowledge*. This manifests not just in asymmetry of access to information, but also in asymmetry of the ability to productively use this information by turning it into knowledge. Mantelero argues that while individuals now have new and varied means to access information, the distribution of information is asymmetric in terms of access to valuable and reliable data as well as to the ability to make use of it, given that

[156] Manzerolle and Smeltzer, 2011, p.327
[157] Hintz et al, 2017, p.732

power over information is concentrated in the hands of a few[158]. Mantelero makes the point that even if we had access to behavioural data it is unlikely that this would make a significant difference to the power imbalance inherent in surveillance capitalism:

> *"A large amount of data creates knowledge if the holders have the adequate interpretation tools to select relevant information, to reorganize it, to place the data in a systematic context, and if there are people with the skills to define the design of the research and give an interpretation to the results generated by Big Data analytics"[159].*

In a similar vein, Innis talked about 'monopolies of knowledge'[160], by which power is maintained through the control of knowledge. Heyer and Crowley observe that these lead to "*inequitable distribution of power and wealth*"[161]. As Lightfoot and Wisnieski argue, informational asymmetries are essential in maintaining power yet may come with severe consequences for some[162]. Reviewing the economic literature on informational asymmetries, they conclude that they are "*insidious for both a variety of specific actors and for broader society*"[163], with only a select few benefiting and at great cost to the many, and argue that in surveillance the asymmetry of information determines the possession of power[164]. This echoes the argument put forward by Lyon that surveillance "*usually involves relations of power in which watchers are privileged*"[165]. Aside from the fact that corporations generally control the platforms that allow them to provide nudges to guide our behaviour, only corporations, not consumers, are practicably able to invest in the equipment and research needed to properly gather, store, and analyse the large quantities

[158] Mantelero, 2014, p.24
[159] Mantelero, 2014, p.24
[160] Innis, 1989
[161] Heyer and Crowley, 1989, p.xvii
[162] Lightfoot and Wisnieski, 2014, p.215
[163] Lightfoot and Wisnieski, 2014, p.218
[164] Lightfoot and Wisnieski, 2014, p.223
[165] Lyon, 2007, p.15

of behavioural data produced by the multitude of digital citizens in the logic of algorithmic governmentality, and so only corporations, not consumers, are capable of producing knowledge from this information and exerting power and control.

Dataveillance, like all surveillance, therefore relies on an asymmetry of knowledge in which the watchers hold a privileged position in terms of both their access to information and their ability to turn this information into knowledge in order to be successful. This imbalance determines that power is possessed by the corporation, not the consumer. Remember that in Chapter 2 we defined power as the capacity to perform a certain act or to bring about a change in behaviour, or the performance of certain behaviour, in another. In this it is clear that the individual holds little power while the corporation holds a lot – in dataveillance, the digital citizen may be to a large extent unaware that their personal and behavioural data is being gathered, how it is turned into profit, that it is often sold to third parties, or who these third parties are. To take Facebook as an example, in truth we know relatively little about its business practices and we know even less about its algorithms, but Facebook 'knows' much about each of its users and is therefore able to attempt to predict and influence their future behaviour for profit. Facebook's knowledge of us is central to its power – the most fundamental informational asymmetry of all in surveillance capitalism is between the visible and knowable computer mediated individual and the invisible and unknowable algorithms that exert control over them on behalf of the corporation. Of course, informational asymmetry is not new to surveillance capitalism – Akerlof, Spence, and Stiglitz were awarded the Nobel Prize in economics in 2001 for their analyses of markets with asymmetric information[166], for example – but the extent of the asymmetry created by a combination of big data, dataveillance, and the global reach of many of these corporations is a unique feature of surveillance capitalism.

[166] Royal Swedish Academy of Sciences, 2001

The wealth of information that can be determined about the digital citizen from the computer mediation of behavioural data gathered through the surveillance of their lives as they move through the digital world allows the individual to be known intimately. And the information about what forms of nudges most effectively influence a given individual's behaviour, which is obtained through the continual experimentation at the heart of hypernudging in the algorithmic governmentality of surveillance capitalism, means that corporations know how to most effectively influence their behaviour. Through this, the algorithms of surveillance capitalism don't just seek to optimise what they show us to match our wants, but they seek also to optimise us as consumers by influencing what we want in the first place by providing nudges to drive behaviour in the way desired. Rather than being the active consumer-citizen engaging in a perpetual process of choice-making in pursuit of their own self-interest, the choice-making of the neo-liberal digital citizen exercising agency as a social and economic actor is thus directed towards the pursuit of the interests of corporations. Surveillance capitalism, then, doesn't just respond to consumer wants – it creates, reinforces, and directs those wants in such a way as to benefit corporations. And it is the informational asymmetry between consumer and corporation inherent in surveillance capitalism that allows this to happen, thus facilitating the appropriation the sovereignty of the consumer.

And we are assumed to be the active consumer-citizen of the neo-liberal ideal despite the fact that the informational asymmetry that exists in surveillance capitalism strips us of power in this way and reduces consumer sovereignty to an artifice. This is because neo-liberalism does not account for asymmetries of knowledge or power[167], but instead places personal responsibility for individual wellbeing firmly with the individual regardless of attenuating circumstances. Indeed, this is a central feature of the neo-liberal concept of the role of the individual within the state[168]. As such it becomes our fault if we as digital citizens fail to fulfil the role of the sovereign consumer actively making choices in our self-interest – if, say, we become knowable and predictable to the extent

[167] Harvey, 2005, p.68
[168] Harvey, 2005, p.68

that corporations can target us with highly persuasive nudges designed to be as effective as they can possibly be at influencing how we exercise our agency as a social and economic actor so as to direct it in the way that is most profitable for corporations. Despite the asymmetries of information that lead to this being possible and which lie beyond our control, we as digital citizens are responsible for failing to pursue our own self-interest at all opportunities. However, there are ways that the digital citizen can go some way towards resisting these practices, which we will now move on to discuss.

3.3 | Resisting Surveillance Capitalism

As Foucault says, "*Where there is power, there is resistance, and yet, or rather consequently, this resistance is never in a position of exteriority in relation to power*"[169]. Resistance is a part of the network of power relations that we recognise in a governmentality analysis, so if we wish to get a fuller picture of surveillance capitalism then it is not enough just to discuss its governmentality and the role of the individual as desired by corporations, but we should also talk about the ways that it can be resisted. We will do this by discussing how people are attempting to engage in small, everyday acts of resistance. Scott describes 'everyday resistance', which involves "*tacit* de facto *gains*" as opposed to the "*formal* de jure *recognition of those gains*" sought by other forms of resistance[170]. Everyday resistance techniques are typically small scale, relatively safe, promise material gains, and require little or no formal coordination, but do require some degree of cooperation and can become a wider pattern of resistance[171]. The key characteristic of everyday resistance, according to Scott, is concealment either of the identity of the resister or of the act of resistance itself[172]. Vinthagen and Johansson, following from Scott, talk of everyday resistance as being that which takes the form not of demonstrations, rebellions,

[169] Foucault, 1990, p.95
[170] Scott, 1990, p.34
[171] Scott, 1989, pp.35-36
[172] Scott, 1989, p.54

or other typically public and collective forms of resistance, but "*how people act in their everyday lives in ways that might undermine power*"[173]. Much of the resistance to surveillance capitalism takes this form, so it is this everyday resistance on which we will focus.

A variety of ways have sprung up in which people can engage in everyday resistance to the algorithmic governmentality of surveillance capitalism. We will look at a two of these in order to illustrate how digital citizens are engaging in resistance. The first is the spread of ad-blocking; the second is the 'do not track' movement. While there are other forms of resistance to surveillance capitalism, such as users deleting their accounts, these are in practice quite limited in effect. Account deletion does not prevent tracking and surveillance of behaviour – Facebook, for example, is known to track even non-users around the internet[174], and Google's targeted advertising, based on surveillance, is pervasive even beyond Google's services (provided by DoubleClick, a Google subsidiary). Managing privacy settings has, for the most part, been a way for users to protect their privacy in relation to other users rather than in relation to the corporations who provide the services in question (built-in options for limiting surveillance have generally been far more limited, reflecting the fact that surveillance is an intrinsic feature of these services). As a result, it is on ad-blocking and do-not-track – which can potentially bring more tangible gains – that we will focus. We will look at these in turn, and will also discuss ways in which surveillance capitalism companies have attempted to overcome these forms of resistance.

3.3.1 | Ad-blocking

Ad-blocking is perhaps the most prevalent form of resistance to surveillance capitalism – as of 2016 an estimated 615 million devices ran some form of ad-

[173] Vinthagen and Johansson, 2013, p.2
[174] Toor, 2016

blocking software[175], potentially costing advertising companies up to $27 billion globally by 2020 in lost revenue (about 10% of their total revenue)[176].

Ad-blocking generally speaking only works on the web, and in most cases only on the desktop web (although some mobile browsers with built in ad-blocking, such as Samsung's Android browser[177] do exist – it is notable, however, that when Samsung first released a browser with ad-blocking capabilities Google tried to remove it from the Android Play Store before eventually restoring it[178], highlighting how Google's control of the Android platform, by far the dominant smartphone platform globally, can be leveraged to suit their ends). The popular ad-blocking software AdBlock, for example, works by inserting code into websites as they are downloaded which prevents adverts from appearing[179]. This is in theory a stealthy form of resistance, in that, as blocking occurs on the user's computer, websites and ad providers do not know when it is occurring. Some websites, however, seek to detect when ad-blocking software is being used and to circumvent it or to prevent access to the site, with varying degrees of success. To the extent that it is possible, concealment of the act of ad-blocking, one of the key features of everyday resistance as identified by Scott, is therefore vital for the success of ad-blocking software. To this end, researchers have developed what they call 'perceptual ad-blocking'. They claim that this will end the 'arms race' between ad-blockers and the companies that try to circumvent them by employing a number of innovative techniques, including by focusing on identifying ads by appearance rather than by trying to spot code in websites that may carry them and by borrowing techniques from malicious software that seeks to escape detention from anti-virus software and applying them to trying to avoid detection by anti-ad-blocking scripts[180]. Whether their claims stand up, of course, remains to be seen.

[175] PageFair, 2017, p.5
[176] Juniper Research, 2016
[177] Seifert, 31/01/2016
[178] Seifert, 09/02/2016
[179] Cassidy, 2016
[180] Storey et al, 2017

Dataveillance companies have responded to the increasing use of ad-blocking software in a number of ways. On mobile platforms they often encourage users to install and use their apps rather than accessing services through browsers, as within these apps they can provide an environment that is under their control and beyond the reach of ad-blockers without system modifications that require technical knowledge to implement and often void the device's warranty. Google, Microsoft, and Amazon have also been known to pay the creators of ad-blocking software to not block their ads[181]. And Google has proposed to include its own ad-blocker in its Chrome web browser. This may seem like a counter-intuitive move by a company that makes the vast majority of its profit through online advertising, but the details of Google's proposal reveal that what it is actually trying to do is both protect its business model and strike a decisive blow against competitors.

Google's plan is two-fold – implement an ad-blocker across both desktop and mobile that blocks ads from other companies that don't meet their standards, while also restricting access to websites by users of third party ad-blockers unless they are willing to pay a fee (a proposal that it calls 'Funding Choices')[182]. The internet is by now the most important publishing platform in the world and Chrome is the most used web browser in the world, with a market share of 56% at the end of 2016[183]. Google presents this plan as being for the benefit of users and publishers, but by creating an advertising platform in which ads provided by other companies are blocked unless they meet Google's standards for quality while at the same time restricting access to pages that use Google's ads if the user tries to block them without paying a fee they are attempting not just to break resistance to surveillance capitalism, but also to break competitors who don't conform to Google's rules. In this model Google would be both a leading player in the advertising market as well as the arbiter of which of its competitors' ads should be shown to users. This plan should therefore be understood as nothing less than an audacious attempt to monopolise the

[181] O'Reilly, 2015
[182] Ramaswamy, 2017
[183] Bright, 2017

principle revenue stream of the most important publishing platform in the world. It has already been shown that online ad platforms other than Google and Facebook are struggling to compete – between them, Facebook and Google accounted for nearly half of global digital ad spending and 77% of digital ad revenue growth in 2016[184] – and if their plan is successful and Google cements its position as the primary way to reliably generate revenue in this way then this would give them immense power. In short, they intend to co-opt as-blocking as resistance in order to more completely monetise the flow of information in the modern world and to control access to the resulting flow of capital.

3.3.2 | The 'Do Not Track' Movement

While ad-blocking primarily seeks to prevent adverts from being shown to a user, the do not track ('DNT') movement takes a different approach and seeks to prevent the tracking of users' behaviour across the internet in the first place. Such tracking allows corporations to build up detailed pictures of user behaviour and preferences beyond the confines of their own websites, even when users are not logged into those websites. Facebook, for example, successfully argued in litigation in the United States that it should be permitted to track its users across the internet even after they had logged out as they had no reasonable expectation of privacy[185]. The judge in that case indicated that if users intended to keep their behaviour private then they should implement some form of DNT, whether through a browser extension or otherwise. DNT is itself simultaneously an act of resistance and an act of concealment, as by preventing the gathering of behavioural data it seeks to both disrupt the practices of surveillance capitalism and to conceal the behaviour of the individual.

[184] O'Reilly, 2017
[185] *In re Facebook Internet Tracking* (N.D. Cal. Jun. 30, 2017)

There are various tools that can be used for DNT, including the TrackMeNot[186] and Privacy Badger[187] Chrome extensions. Some ad-blockers, such as AdBlock, have incorporated DNT into their software[188]. Alternative web services that do not track users have also sprung up, for example the search engine DuckDuckGo[189] which seeks to provide an alternative to Google without tracking user behaviour. Beyond these, Apple announced in September 2017 that it intends to implement DNT in its Safari browser in the latest versions of macOS and iOS, leading to accusations from major advertising companies that Apple is sabotaging the economic model of the internet[190]. However, DNT isn't perfect – French researchers have shown, for example, that even with both ad-blocking and DNT users can be identified and tracked by combining aspects of their browsing (for example, the browser and version that they are using, websites that they are logged into, the extensions that they have installed, their time zone, their screen resolution, etc.) into a unique digital fingerprint in order to circumvent DNT[191].

There have been attempts to put DNT on a legal footing, which have inevitably faced opposition. In the US, advertising firms have invoked First Amendment protections of free speech in order to challenge federal rules that attempt to provide for an 'opt-in' approach to user-tracking[192], and in the same challenge Google has argued that web browsing data is not sensitive information that should be protected[193]. Likewise, the Internet Association – whose founding members include Google and Facebook – has come out in opposition to a Bill introduced to Congress that would provide for opt-in tracking[194]. And in 2015 the FCC ruled that websites are permitted to ignore DNT requests sent by browsers[195]. However, in the EU, the European Commission's working party on

[186] See https://cs.nyu.edu/trackmenot
[187] See https://www.eff.org/privacybadger
[188] See https://adblockplus.org/features
[189] See https://duckduckgo.com
[190] Hern, 08/09/2017
[191] See https://extensions.inrialpes.fr
[192] Mandese, 2017
[193] Google, 03/10/2016
[194] Brodkin, 2017
[195] Brodkin, 2015

data protection strongly recommended making DNT compliance mandatory in the proposed ePrivacy Regulation[196]. Article 10 of the proposed Regulation therefore currently requires that web browsers and other software and equipment by default offer an option to opt-out of tracking[197], and amendments to the draft Regulation proposed by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs seek to make DNT the default setting and to ensure a greater degree of user control over tracking where the user chooses to permit it[198]. The law in the US and the EU, therefore, appears to be diverging when it comes to recognition of DNT.

While DNT remains an act of everyday resistance, in that it remains a largely individual effort to achieve *de facto* gains, there is, therefore, a move towards providing for *de jure* recognition of a need to provide protections against tracking. Through this, it is possible that resistance in this form will become more formalised and, perhaps, more effective, although it remains to be seen whether and to what extent such moves will be successful.

3.4 | Conclusion

ICT, the advent of big data, and associated societal developments have led to major changes in the state and in the role that the digital citizen plays within that state. Google and Facebook have led the way in developing new business models and practices allowing them to take advantage of these changes and grow from personal projects in college dorm rooms to become two of the most valuable and most profitable companies in the world in less than two decades, with a global reach and billions of users, and in doing so to spawn an array of other companies that seek to replicate both their practices and their success. Zuboff sees in this the emergence of a new form of capitalism, which she calls

[196] Article 29 Data Protection Working Party, 2017, p.4
[197] Draft ePrivacy Regulation, COM (2017) 10, Article 10
[198] European Parliament, 2017, Amendments 94-100

'surveillance capitalism', in which profit derives from the unilateral surveillance and modification of human behaviour.

In this chapter, and for the first time, surveillance capitalism has been elaborated on and contextualised in relation to key concepts in surveillance studies in order to provide a fuller account of how it operates. Beyond this, and again for the first time, we have connected the three stages of algorithmic governmentality to surveillance capitalism; identified its rationality in the form of a departure from the cycles of accumulation of previous forms of capitalism and based around the mass surveillance, prediction, and modification of human behaviour; and have shown how its technology of power operates by gathering data from the digital citizen, predictive algorithmic analysis of this data when combined with that of millions of others, and the dynamic, highly personalised form of behavioural nudging called hypernudge. And we can recognise that in surveillance capitalism the digital citizen takes on a new role, and have introduced a new concept to account for this – the produsumer, who is commodified and whose labour is exploited in the pursuit of profit. Along the way, we have identified the points at which existing analyses of other forms of capitalism – primarily that of Marx and of others who build on his work – cannot adequately explain either the logic of accumulation of surveillance capitalism or the role of the individual within that business model. What we have, then, is a new form of capitalism emerging in contemporary ICT-driven societies, which requires a new approach.

The development of this new form of capitalism – and this new form of control – should be understood in the context of the neo-liberal societies in which it has primarily taken place. In surveillance capitalism the sovereignty of the individual – in theory the founding principle of neo-liberalism – becomes appropriated through informational asymmetries, allowing the agency of the digital citizen as a social and economic actor engaged in perpetual choice-making as a consumer-citizen to be directed in the way desired by corporations and facilitating the control of the digital citizen by the powerful behaviour prediction and modification tools of algorithmic governmentality. The self-

commodification of the digital citizen in neo-liberal society forms part of and facilitates their commodification as a data profile to be bought and sold in surveillance capitalism. And through pervasive surveillance, every social and economic interaction within the reach of surveillance capitalism becomes behavioural data to also be commodified and bought and sold on the advertising market, empowering the already powerful and enriching the already wealthy at the expense of the rest. As modern life becomes increasingly digital, surveillance capitalism's voracious appetite for data from which to derive profit and its resulting desire to bring as much of human behaviour within its remit means that modern life also becomes increasingly datafied and commodified. Surveillance capitalism therefore represents the commodification of everyday life itself within the marketised neo-liberal state. The neo-liberal form of both contemporary society and contemporary digital citizenship thus facilitates control according to the rationality of this new variety of capitalism.

In the next chapter we will see how the collection and storage of vast quantities of data in surveillance capitalism is taken advantage of by the State as it seeks to extend its control over the new online world, demonstrating how not just the functioning of the public and private are increasingly intertwined and overlapping in the digital, but also how the forms of control to which the digital citizen is subjected in the online modern world are intertwined and overlapping.

Chapter 4 | The Digital Panopticon: State Surveillance in the Online World

In the preceding chapters we saw how the spread of ICT and the neo-liberal nature of digital engagement has opened the individual up to new forms of dataveillance-based control as corporations seek the commodification of life in pursuit of profit. In this chapter we will see how the State has taken advantage of technological developments and this role as a digital citizen, as well as of the surveillance apparatus of surveillance capitalism, in order to implement its own dataveillance-based forms of control so as to uphold the existing order in the name of security, and in doing so has fundamentally remade the relationship between the digital citizen and the State.

In May 2013 the existence of global online surveillance networks operated by the NSA in the US and GCHQ in the UK was revealed as a result of the deliberate leaking of classified information by former CIA employee and NSA contractor Edward Snowden[1]. Snowden was motivated primarily by a desire to make public what he considered to be abuses of power[2]. There are a range of legal, privacy, and democratic concerns raised by this kind of surveillance. While some aspects of the NSA's activities, for example, have legal authorisation under the Foreign Intelligence Surveillance Act 2001, much of what the NSA has been engaged in may not[3] and aspects of GCHQ's operations have subsequently been found to be unlawful[4].

In the US, the NSA operated the PRISM programme, among others, and, in the UK, GCHQ operated Tempora, primarily, and others[5]. That security and

[1] Greenwald and MacAskill, 07/06/2013; Gellman and Poitras, 2013; Landau, 2013
[2] MacAskill, 10/06/2013
[3] Bajaj, 2014, pp.583
[4] *Liberty v Foreign Secretary and others* [2015] UKIPTrib 13_77-H; *Privacy International v Foreign Secretary and others* [2016] UKIPTrib 15_110-CH, *Tele2 Sverige AB v Post-och telestyrelsen, Secretary of State for the Home Department v Tom Watson and others* [2017] 2 WLR 1289
[5] Bauman et al, 2014, p.122

intelligence agencies ('SIAs') engage in extensive surveillance of the internet has long been known, and there have for some time been legal regimes in place to allow for such surveillance to an extent. But the programmes revealed by Snowden were of such sophistication, scale, and reach that they surprised even seasoned observers[6] (it has been suggested that even those who work for other SIAs were surprised at the extent of the NSA and GCHQ's activities[7]). It was immediately obvious that the details of these programmes involved, as Bauman et al put it,

> *"significant transgressions of established understandings of the character and legitimacy of those institutions concerned with security and intelligence operations … some revelations seem to confirm long-term transformations in the politics of states … and in the institutions and norms established in relation to democratic procedures, the rule of law, [and] relations between state and civil society"[8].*

In short, the surveillance programmes that have been secretly put in place to monitor the digital world that digital citizens have been encouraged to take part in constitute a serious and significant break from preciously accepted societal, political, and legal norms, and they raise concerns about fundamental legal principles including the presumption of innocence and freedom of expression.

As long ago as 1995 Stephen Gill argued that attempts to embed a more systematic form of neo-liberal discipline and surveillance were growing[9], and he warned that as technology became more sophisticated it would increasingly be used to surveil and impose social control in order to reduce the individual to a pliant, obedient subject of the neo-liberal state[10]. The explosive growth since then in the use and sophistication of ICT has allowed the State to adopt

[6] Bauman et al, 2014, p.122
[7] Bajaj, 2014, p.582
[8] Bauman et al, 2014, p.122
[9] Gill, 1995, p.42
[10] Gill, 1995

surveillance measures that would otherwise have been impossible both in extent and in reach. The programmes operated by SIAs move this surveillance from something targeted against suspected criminals or terrorists, to something that is exercised over whole populations and, indeed, the whole planet[11].

In this chapter we will first describe the surveillance programmes revealed by Snowden and show how they form a digital panopticon with a new technology of power of algorithmic panoptic uncertainty, and will link these with the practices of surveillance capitalism; then we will look at what this means for the digital citizen in terms of their relationship with the state through the fundamental norms of the presumption of innocence and the right to freedom of expression; and finally we will discuss the security rationality behind these practices. In all, we will identify the governmentality of the digital panopticon, facilitated by ICT, which seeks to translate rationalities of security into reality and maintain the neo-liberal order.

4.1 | The Digital Panopticon

We will first look at how GCHQ and the NSA's programmes operate in practice and will then identify them as constructing a digital panopticon in which the digital citizen is permanently observable and, therefore, amenable to control.

4.1.1 | Surveillance in Action

There are two primary ways by which online surveillance is undertaken in the NSA and GCHQ programs – the first being Xkeyscore and similar systems involving the bulk interception of communications, and the second being PRISM and similar programs involving the acquisition of data from surveillance capitalism and communications companies as well as equipment interference. We will deal with each of these in turn.

[11] Bauman et al, 2014, p.122

Communications Interception

The first is bulk interception through Xkeyscore and similar systems[12]. This involves the placing of interceptors on the data cables that connect countries and continents and the collection of the vast quantities of both content and, crucially, metadata that pass through them. Metadata is the 'who', 'when', 'where', and 'for how long' of data rather than the content of a communication itself – a common analogy is that metadata is the envelope rather than the letter, which is content. It has been pointed out[13] that metadata can provide more information and more readily analysed data on someone than content:

> *"Law enforcement and intelligence officials … prefer metadata, not just [for] how revealing it is in an individual case, but because they can use their powerful analytic tools. They can mine metadata in a way that they really can't content. People can disguise what they're talking about when they're having conversations with each other, but metadata doesn't lie. Metadata says who contacted who, when and for how long"*[14]

According to former NSA General Counsel Stuart Baker, "*Metadata absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content*"[15].

Xkeyscore is the most technologically advanced aspect of the NSA and GCHQ's surveillance. Other programmes funnel data to Xkeyscore implementations, and the system is used by all members of the 'Five Eyes' group of countries (the UK, USA, Canada, Australia, and New Zealand, who since 1946 have agreed to share intelligence and cooperate in surveillance). Xkeyscore allows for the collection

[12] A redacted NSA presentation detailing how to use Xkeyscore is available via the Guardian at http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation
[13] Kadidal, 2014, pp.444-456; Zuckerman, 2013
[14] Democracy Now, 2013
[15] Rusbridger, 2013

of content and metadata and the real time searching of this data by analysists[16], allowing communications to be monitored as they are happening. This is used to find out what a given target is doing online at any given point in time[17]. The British implementation of Xkeyscore, codenamed Tempora, is alone reported to involve over 200 interceptors on the internet backbone cables running from the British Isles to the rest of the world[18], and UK telecommunications operators including BT and Vodafone are reported to have given GCHQ access to their cables[19]. Tempora is the biggest contributor to pooled content and metadata repositories held by the Five Eyes, and is estimated to be bigger than all other implementations of Xkeyscore combined[20].

As bulk interception of this kind involves all data, regardless of source or destination, the distinction between monitoring the communication of a State's own citizens and of foreign nationals is lost[21]. Instead, everyone is rendered visible and potentially under suspicion[22], casting doubt on claims made three months before the Snowden leak by the US Director of National Intelligence, who testified to the US Senate that the NSA had not knowingly collected any data on American citizens[23]. The fact that all data is collected also means that legal safeguards intended to limit the ability of SIAs to conduct mass surveillance of British citizens in the UK are undermined. While the Regulation of Investigatory Powers Act ('RIPA') states that internal warrants (for bulk interception of communications entirely within the UK) must be targeted at a specific address or a specific person, external warrants (for interception of communications coming to or leaving the UK) are not subject to this limitation[24]. The Investigatory Powers Act ('IPA'), which will replace RIPA, permits bulk communications interception for what it calls "*overseas-related*

[16] Kadidal, 2014, pp.456-457
[17] https://theintercept.com/gchq-appendix/
[18] Bauman et al, 2014, p.122
[19] https://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq; presumably authorised under Regulation of Investigatory Powers Act 2000 ('RIPA 2000') ss.11-12
[20] http://www.spiegel.de/media/media-34090.pdf
[21] Bauman et al, 2014, p.125
[22] Bauman et al, 2014, pp.125-126; see Chapter 4.2.2
[23] Landau, 2013, pp.54-55
[24] RIPA 2000 s.8

communications"[25], which, like external warrants, apply to communications coming to or leaving the UK[26]. Since a large proportion of internet traffic will be going to or coming from servers located outside the UK, most online activity by users located in the UK could be caught by an external warrant under RIPA or a bulk interception warrant under IPA and thus would come within the reach of Tempora.

External warrants under RIPA are issued by the Home Secretary upon request from SIAs without requiring judicial approval[27], but bulk interception warrants under IPA do require the approval of a Judicial Commissioner[28] (the Judicial Commissioners are a team of current or former judges led by an Investigatory Powers Commissioner and appointed by the Prime Minister to oversee the exercise of surveillance powers under IPA[29]). As with most of these programmes, the legality of Tempora is contested. While the Investigatory Powers Tribunal ('IPT') has found that the use of RIPA external warrants for similar purposes is lawful[30], the European Court of Human Rights is considering a case brought by Big Brother Watch and others, who contend that Tempora, as authorised under RIPA, is incompatible with Article 8 ECHR[31].

Unrelated to Xkeyscore, police and SIAs also obtain phone calls, text messages, and other video and audio communications by intercepting mobile phone communications with a man-in-the-middle attack[32]. Police and SIAs in the US[33] and in the UK use 'Stingray' devices that enable them to set up a dragnet to catch nearby mobile communications by simultaneously impersonating cell towers of up to four networks across the full 2G/3G/4G spectrum. Stingrays, more properly known as IMSI catchers, allow them to track mobile devices and to access content and metadata transmitted by all devices that unwittingly connect

[25] IPA 2016 s.136(3)
[26] IPA 2016 Pt.6 c.1
[27] RIPA 2000 ss.7-8
[28] IPA 2016 s.138
[29] IPA 2016 Pt.8 c.1
[30] *Liberty* [2015] UKIPTrib 13_77-H
[31] Big Brother Watch, 2017
[32] Bauman et al, 2014
[33] Farivar, 2015; Biddle, 12/09/2016

to the fake cell tower, whether the operator of the device is suspected of an offence or not. UK police forces that appear to own Stingray (or Stingray-like) devices include the Metropolitan Police, West Midlands Police, Avon and Somerset Constabulary, West Mercia Police, Warwickshire Police, Staffordshire Police, and possibly others[34]. Journalistic investigations have detected that they are used in at least 20 locations in London[35], including at the Palace of Westminster[36]. The strength of the legal basis for the use of Stingray devices by police forces in the UK, which is claimed by the Government to be authorised under the Intelligence Services Act[37], the Police Act[38], and RIPA[39], remains unclear.

Data Acquisition

The second approach taken is the PRISM programme, and similar. This involves accessing data held by technology companies and telecommunications operators, as well as systematically weakening encryption standards and installing backdoors in networking equipment so as to facilitate acquisition. This data is then fed into over 500 data repositories distributed in approximately 150 locations around the world[40] and again allows for real time searching of this data by analysts using Xkeyscore's systems and collation and analysis through other systems.

Third Parties

PRISM, in part, involves regularly forcing surveillance capitalism corporations to provide personal and behavioural user data to the NSA without the knowledge or consent of users[41]. As users provide data to the corporations who

[34] Aviram, 2016; O'Neill, 2014
[35] BBC News, 10/06/2015
[36] Bryant, 2016
[37] Intelligence Services Act 1994
[38] Police Act 1997
[39] House of Lords Hansard, 11/11/2014
[40] http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, slides 3-5
[41] Greenwald and MacAskill, 07/06/2013; Bauman et al, 2014, p.123

subsequently provide this data to intelligence agencies they are unwittingly complicit in their own surveillance. We have seen already[42] that surveillance capitalism involves datafying and commodifying the digital citizen in order to sell them as data profiles on the advertising market and generate profit, and this data is also of interest to SIAs as they seek to exercise control over populations. And not only are surveillance capitalism corporations providing their data to SIAs, but as users of their services digital citizens make the SIAs' job easier by delineating themselves into groups of shared interests and shared connections. In effect, they perform the first sorting of intelligence data themselves:

> *"The clustering of groups who like the same music or movies or sports is achieved by the users themselves, before the work … of splitting them up using algorithms begins. Social media continue to be hugely popular, and while they can be a potent means of shaping political opinion and protest, they also provide the raw materials of data for both corporations and, as Snowden has shown us, police and intelligence agencies."*[43]

Various legal powers in both the US and the UK underpin this. According to court documents, Yahoo attempted to fight NSA demands for data but was threatened with a $250,000 per day fine if it did not comply, with the fine doubling every week that non-compliance continued[44]. In the US, the Supreme Court has ruled that disclosure of an individual's data by a corporation that holds it to a third party is not protected by the Fourth Amendment[45] – this doctrine is widely criticised[46]. In the UK, IPA provides for warrants allowing SIAs to obtain personal data, including sensitive personal data, in bulk from third parties[47]. While it has been public knowledge that the NSA acquired data from technology companies, the use of bulk personal data acquisition powers by UK SIAs authorised under previous legislation was only admitted to in March

[42] Chapter 3
[43] Bauman et al, 2014, p.142
[44] Rushe, 2014
[45] *Smith v Maryland* 442 U.S. 735 (1979)
[46] Kadidal, 2014, pp.447-448
[47] IPA 2016 Pt.7 – 'personal data' here has the same meaning as in the Data Protection Act 1998

2015[48] (the IPT ruled that these powers did not comply with ECHR prior to being admitted to, but did comply once their existence was known[49]). And documents released to Privacy International in September 2017 as part of proceedings brought by them before the IPT revealed that GCHQ has been acquiring personal data in bulk from social media companies, with the Investigatory Powers Commissioner apparently unaware that this was taking place[50]. Under a proposed agreement between the US and the UK, US-based technology companies would be obliged to provide data to UK SIAs[51].

IPA also provides for the systematic retention of bulk communications data[52] (i.e. metadata, rather than content) by ISPs, including mobile operators, with retained data on specific individuals to be provided to certain public authorities – including police and SIAs – upon request[53]. The data to potentially be retained is wide-ranging[54], and includes, for a home broadband connection, as well as the hostname of each website that a user has visited (the hostname is the address of the website visited rather than the address of the specific webpage on the website visited – e.g. 'www.example.com' rather than 'www.example.com/index.html'), 17 different items for every single data communication covered by a retention notice including, inter alia, the name, address, and phone number of the customer holding the account with the ISP; email addresses linked to the account; bank account information used to pay for and billing information relating to the account; the username and password for the account; and a variety of technical details that would enable the identification of the specific devices involved. For a mobile connection, network providers may also be required to retain information identifying the geographical location of the device including network maps and details of the network masts that the device is connected to. This aspect of IPA, which is popularly known as the 'snooper's charter' and which replaces powers under

[48] *Privacy International* [2016] UKIPTrib 15_110-CH at [13]
[49] *Privacy International* [2016] UKIPTrib 15_110-CH at [101]
[50] Privacy International, 2017
[51] Murgia, 2017
[52] IPA 2016 Pt.4
[53] IPA 2016 Pt.3
[54] Joint Committee, HL 93/HC 651, pp.515-517

earlier legislation that were found to be incompatible with EU law[55], also appears to itself be incompatible with EU law[56]. IPA further gives British SIAs the power to require that UK telecommunications operators – including ISPs, telephone companies, and mobile phone networks – provide communications data to them in bulk upon request[57], rather than in relation to specific individuals, a power that was previously exercised under RIPA[58] and earlier legislation[59].

Equipment Interference

As part of PRISM, the NSA has also engaged in a systematic assault on encryption standards, and collected content and metadata directly from backdoors in network equipment. In this, they have infiltrated standards-setting bodies so as to weaken standards and installed backdoors in firewalls, hard drives, network infrastructure, and encryption products in order to facilitate their access to networks and devices[60]. Data acquired this way is fed into other systems including Xkeyscore. The NSA's Bullrun programme, part of PRISM, aims to break encryption and allow the NSA access to data encrypted using protocols such as HTTPS, voice-over-IP, and Secure Sockets Layer (SSL), which are used to protect online shopping, banking, and business, among many other things. According to Schneier, "*By deliberately undermining online security in a short-sighted effort to eavesdrop, the NSA is undermining the very fabric of the internet*"[61]. In 2016 a set of exploit tools apparently originating inside the NSA appeared for sale on the dark net, seemingly having been accessed and then copied by hackers[62]. A further set of tools, released by the same group and again apparently originating inside the NSA, appeared on the dark net in 2017[63] and

[55] Data Retention (EC Directive) Regulations 2009; Data Retention and Investigatory Powers Act 2014
[56] See Chapter 6.3 for a full analysis of the compatibility of communications data retention and disclosure under Parts 3 and 4 IPA with EU law
[57] IPA 2016 Pt.6 c.2
[58] RIPA 2000 Pt.1 c.2
[59] Telecommunications Act 1984 s.94
[60] Bajaj, 2014, p.583
[61] Ball et al, 2013
[62] Groll, 15/08/2016
[63] Goodin, 14/04/2017

was used in an attack across 74 countries which severely impacted the NHS in May 2017[64]. As Green points out,

> *"The danger of these exploits is that they can be used to target anyone who is using a vulnerable router … So the risk is twofold: first, that the person or persons who stole this information might have used them against [the United States] … And now that the exploits have been released, we run the risk that ordinary criminals will use them against corporate targets"[65].*

In the UK, IPA provides for warrants to conduct bulk equipment interference[66] for overseas-related communications[67]. These warrants are new to IPA, with bulk equipment interference having not previously been undertaken by any of the UK SIAs[68], and have been described as "*bulk hacking*" by the Open Rights Group[69]. They would allow security and intelligence agencies to be granted a warrant to access content and metadata from "*any equipment*"[70], without restriction[71], in order to determine whether anything suspicious has occurred. According to the Government these powers can be used speculatively to access all devices in a particular area so as to identify potential targets of interest[72]. IPA also provides that technology companies can be required to maintain the technical capability to lift encryption on communications and stored data where requested or to provide a backdoor to SIAs, provided the Government issues regulations fleshing out the legal framework for this[73]. The Government has consulted on regulations[74], signalling its intention to use this power, and in the wake of terrorist attacks in the UK during 2017 has repeatedly indicated that it

[64] Perlroth and Sanger, 2017
[65] Biddle, 19/08/2016
[66] IPA 2016 Pt.6, c.3
[67] IPA 2016 s.177
[68] Anderson, 2016, p.103
[69] Johnson-Williams, 2016; Liberty calls BEI "*mass hacking*" (Liberty, 2016)
[70] IPA 2016 s.177(1)
[71] Operational requirements would presumably determine the extent of the equipment interference
[72] Home Office, 31/10/2015
[73] IPA 2016 ss.253-258
[74] Smith, 2017

wants messaging services like WhatsApp, which uses end-to-end encryption, to implement backdoors so that the SIAs can access content[75].

Police in the UK are also known to have been downloading data from people's phones – including call records, text messages, and contact lists, as well as any other data stored on the phone – when they have been stopped for questioning under Schedule 7 of the Terrorism Act 2000 and sending it to GCHQ as part of a programme called Phantom Parrot[76].

The Black Hole

Much of GCHQ and the NSA's collected data flows into the Black Hole repository[77], which is at the heart of GCHQ's surveillance and from which GCHQ's Karma Police programme draws its data. In operation since at least 2009, Karma Police creates a profile of the browsing habits of every visible user on the internet without any distinction as to nationality and without any apparent oversight[78]. GCHQ themselves describe Black Hole as the world's biggest data mining programme[79], and by 2012 it was collecting over 50 billion records every day[80]. The operation of the Karma Police system in processing Black Hole data is summarised as follows:

> "*One system builds profiles showing people's web browsing histories. Another analyzes instant messenger communications, emails, Skype calls, text messages, cellphone locations, and social media interactions. Separate programs were built to keep tabs on 'suspicious' Google searches and usage of Google Maps*"[81]

[75] Sparrow, 2017
[76] Gallagher, 2017
[77] Gallagher, 2015
[78] Gallagher, 2015
[79] Gallagher, 2015
[80] Gallagher, 2015
[81] Gallagher, 2015

Using the Mutant Broth system, GCHQ analysts can input an unidentified user's IP address and return identifying information including email addresses, usernames, and passwords from Black Hole (likewise a known individual's email address can be inputted to return their last known IP address)[82]. GCHQ also has a related system called Samuel Pepys, which provides a "*near real-time diarisation*" of communication and web browsing traffic linked to a particular IP address and which is used to find out "*what is my target doing online right now?*"[83]. The sophistication and extent of bulk content and metadata collection and collation and tracking of the activities of such a large number of people undertaken by GCHQ and the NSA would have been inconceivable in the pre-digital era.

4.1.2 | Constructing the Panopticon

The panopticon was a plan for a prison put forward by the philosopher Jeremy Bentham in the 1790s, purporting to be a liberal reforming institution, in line with Bentham's broader philosophy, which would remake prisoners as better citizens. Although it was never constructed, the principles applied in the panopticon have been of great significance in studies of power, control, and surveillance – Foucault described it as "*the diagram of a mechanism of power reduced to its ideal form*"[84], writing that "*whenever one is dealing with a multiplicity of individuals on whom a task or a particular form of behaviour must be imposed, the panoptic schema may be used*"[85].

At the heart of the panopticon is visibility[86]. As Foucault wrote, in the panopticon "*visibility is a trap*"[87]. Cells would be arranged in a circular fashion around a central observation tower, with the sides facing the tower covered in bars but no wall, and all prisoners and all of their actions would be visible in

[82] Gallagher, 2015
[83] https://theintercept.com/gchq-appendix/
[84] Foucault, 1991, p.205
[85] Foucault, 1991, p.205
[86] 'Panopticon' comes from the ancient Greek *πανόπτης* (*panóptis*) meaning 'the all-seeing' (http://www.oed.com/view/Entry/136920#eid32182939)
[87] Foucault, 1991, p.200

their cells to the guards in the tower and could therefore be observed at any time. However, the guards, ensconced in the tower and hidden behind blinds, would themselves be invisible to the prisoners. All prisoners could be watched at any time, but they would go about their business without ever knowing for sure whether the guards were watching *them* in particular or not. As Foucault puts it, the prisoner is totally seen but never sees[88]: "*he is the object of information, but never a subject in communication*"[89]. In this, the crowd of prisoners is abolished and replaced by a collection of separated individuals who can be numbered and supervised[90]. It would not be necessary to constantly observe all prisoners – the "*asymmetrical gaze*"[91] creates what we could call 'panoptic uncertainty', the knowledge that at any point in time you *could* be being watched and the uncertainty of never knowing for sure whether you are or not.

Uncertainty is, in theory, enough to regulate behaviour and is key to the effectiveness of the panopticon[92]. Bentham felt that "*Punishment, even in its most hideous forms, loses its odious character, when bereft of that uncertainty*"[93]. Utilising uncertainty to exert control is his true innovation[94] and the primary control mechanism of panoptic forms of surveillance. As Foucault puts it, "*the major effect of the Panopticon [is] to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power*"[95]. Harold Innis talked about 'monopolies of knowledge'[96], by which power is maintained through the control of knowledge, and Heyer and Crowley observe that these lead to "*inequitable distribution of power and wealth*"[97]. This imbalance of knowledge created by the imbalance of visibility leads to an imbalance of power between the watched and the watcher inherent in all surveillance, but it is

[88] Foucault, 1980, p.202
[89] Foucault, 1991, p.200
[90] Foucault, 1991, p.201
[91] Lyon, 1994, p.65
[92] Lyon, 1994, p.65,
[93] Bentham, 1843
[94] Lyon, 1994, p.65
[95] Foucault, 1991, p.201
[96] Innis, 1989
[97] Heyer and Crowley, 1989, p.xvii

through the internet and surveillance of our everyday online lives that this imbalance is writ large.

And the digital panopticon adds an extra dimension – not only can we not know *when* we are being watched, we also can't know *how* we are being watched. Where in Bentham's panopticon prisoners knew that they could be watched from the central tower, algorithmic opacity means that the tools by which SIAs make sense and use of the vast quantities of surveillance data available to them are hidden in black boxes, invisible and unknowable to those subject to their control. And just as it is impossible to know how these systems operate, it is also impossible to know what information about any given individual has been or could be inferred or predicted by algorithmic analysis, whether by surveillance capitalism corporations before they pass data to SIAs or by the SIAs themselves. By informating, smart machines turn informer, betraying the details of selves and lives to those who seek panoptic control. In our governmentality analysis we can locate this new *algorithmic panoptic uncertainty* - distinguished from previous forms of panoptic uncertainty in that algorithmic opacity and the power of predictive analytics elevates the imbalance of knowledge between the watched the watcher to a new level – as a technology of power that seeks to render the watched amenable to the control of the watcher according to the rationality being pursued.

In the digital world surveillance no longer needs to be undertaken up close. With the internet and other modern forms of communication such as mobile phones it can be done at any distance, and far more data about the individual can be obtained than ever before. In large part this is because the nature of communication devices themselves has changed – mobile and smart phones can disclose far more personal and communications data than stationary phones ever could, for example[98]. But the fact that surveillance capitalism corporations also provide to SIAs the personal and behavioural data that they have obtained through consumer surveillance demonstrates that while it might seem that the

[98] Landau, 2013, p.56

panspectric surveillance undertaken by corporations and discussed in Chapter 3 and the panoptic surveillance undertaken by the State and discussed here are discrete regimes, they are in fact linked. While they exert control over the individual in different ways, in pursuit of different goals, and with different effects, consumer surveillance feeds into State surveillance. The extensive dataveillance apparatus of surveillance capitalism, making use of algorithmic governmentality to control the digital citizen as a social and economic actor in pursuit of commercial rationalities, is thus brought within the reach of the State in the digital panopticon, and expansions in the extent of consumer surveillance represent commensurate expansions in the extent of State surveillance. This may have major implications as IoT devices feeding data back to corporate databases become the norm and as cameras as microphones become embedded in an increasing number of every day devices, thereby creating not just an internet of *things* but an internet of *eyes* and *ears*, and the temptation for the State to bring this data even further within its control will grow.

In our analysis we can recognise the digital panopticon as a governmentality, involving the technology of power of algorithmic panoptic uncertainty and seeking to exert control over the digital citizen. As we know from Chapter 2, every governmentality involves three elements – a rationality, a technology of power, and a subject. We will move on now to discuss the effect of this governmentality on its subject – the digital citizen – and their relationship with the State, before discussing its rationality as it is employed in western neo-liberal societies.

4.2 | The Digital Citizen in the Digital Panopticon

The digital panopticon is, of course, not the first time that a State has undertaken mass surveillance of its population, but in the governmentality of the digital panopticon the State no longer requires the citizen to be an active participant in that surveillance. The digital citizen instead takes on a passive role, while work that was once done by people is increasingly done by machines

that watch and listen, that record and transmit, and that predict and inform. The Stasi, for example, had perhaps the most notorious State surveillance regime of all and compiled extensive records on many East Germans, but this relied on the co-operation of the public in divulging information and reporting their peers, and required huge numbers of staff. The Stasi employed 100,000 of East Germany's 16 million people, and up to another 200,000 were used as 'informal collaborators' by 1989[99]. It therefore relied, directly or indirectly, on up to 300,000 people feeding it information and analysing that information. This would be equivalent to the NSA employing more than 6 million Americans – it is estimated to employ around 100,000[100], yet processes orders of magnitude more data. The Stasi also faced a significant problem – how to organise, store, and make use of such large quantities of information held in paper records.

The digital panopticon avoids both of these problems – data can be systematically collected, sorted, and accessed without relying on the active co-operation of the public, and algorithmic systems allow intelligence analysts to look up virtually any individual at will in real time. The NSA said in 2013 that it 'touches' 29 petabytes of global data every day[101] and, while even with modern computing power it struggles to process all of it[102], its job is much easier than that of the Stasi. While the Stasi had 10,000 operatives dedicated to transcribing telephone conversations, now, as Kadidal points out, an array of smartphones could do the same task[103]. Foucault felt that the panopticon "*makes it possible to perfect the exercise of power … because it can reduce the number of those who exercise it, while increasing the number of people on whom it is exercised*"[104], and when panoptic uncertainty is combined with big data and predictive analytics to create algorithmic panoptic uncertainty this is amplified to an unprecedented degree. This new passive role removes the digital citizen from this aspect of the

[99] Kadidal, 2014, p.457
[100] MacAskill et al, 06/06/2013
[101] Jarvis, 13/08/2013; to put this into context, 1 petabyte is the equivalent to 223,000 DVDs of storage at standard 4.7 Gb size (or 749 million floppy disks). Kadidal estimates (2014, pp.457-458) that it would be both possible and affordable for the NSA to store all 300 petabytes of US-only traffic per year
[102] Angwin, 25/12/2013
[103] Kadidal, 2014, p.457
[104] Foucault, 1991, p.206

cycling of power through the differentiated polity of the neo-liberal state. Where before an army of informers was required to track, record, and feed data back to the State, now behaviour is tracked and recorded by devices as people go about their day-to-day lives and algorithmic analysis reveals otherwise unknown information about the individual. Rather than playing a role in the cycling of power as active participants in surveillance, the population is now reduced to pliant subjects of that power.

While the digital panopticon does not signal a move to the kind of totalitarian police state seen in some countries where mass surveillance is employed in order to uphold an autocratic or dictatorial regime, it does raise important questions about the nature of surveillance and the role of the individual in a free and democratic society. Bell et al note that the State sees the acquisition of our data as its right, and citizens open to punishment for resisting[105]. Ultimately there is a tension between the concept of the sovereign individual free to pursue their own self-interest as they see fit without State interference in their rights and liberties – which in theory lies at the heart of neo-liberal society – and the role of the State in protecting security and society. As Bauman et al point out, this tension is often depoliticised by reference to the 'need' to strike a 'balance' between liberty and security[106], often by those who wish to resolve the tension in favour of security, but the decisions to circumscribe liberty in pursuit of security and to what extent to do so, while perhaps desirable and understandable to a degree given the very real threats faced by western societies, are in fact political choices made in pursuit of certain rationalities. In the view of Ball et al, "*talk of balance between 'security' and 'liberty' is highly misleading … liberty is an integral component of what makes security for citizens. Without liberty there is no citizenship, and there is only insecurity. Security is not a trump card*"[107].

[105] Select Committee on the Constitution, HL Paper 18-II, p.24
[106] Bauman et al, 2014, p.137
[107] Select Committee on the Constitution, HL Paper 18-II, p.24

The digital panopticon resolves this tension in favour of security in a way that challenges norms of democratic citizenship in relation to the presumption of innocence and freedom of expression, and ultimately may undermine the health of democracy itself. Murakami Wood argues that "*We exist in a society of a kind of tacit social contract where we expect to be free and to have those freedoms protected and the main reason for security is to protect our rights to go about our daily business unhindered. Where that protection starts to remove those freedoms themselves, I think that tacit contract is challenged*"[108]. Foucault wrote that through the control mechanism of uncertainty those within the panopticon are "*caught up in a power situation of which they are themselves the bearers*", that they "*assume responsibility for the constraints of power*"[109] becoming "*the principle of [their] own subjection*"[110]. The digital panopticon allows power to increase its points of contact[111], and it is in these points of contact that government, as a power interaction that seeks influence an individual's behaviour according to particular rationality, takes place. Through this, citizenship is remade by the technology of power of the digital panopticon, with the digital citizen rendered as a potential criminal, a constantly observed object of suspicion, while fundamental principles of a free and democratic society that exist for the benefit of the citizen are eroded.

4.2.1 | Eroding the Presumption of Innocence

The House of Lords Constitution Committee published a report on surveillance and the citizen in 2009, long before the true extent of mass electronic surveillance was known. The report said that that mass surveillance threatened to undermine basic tenets of the relationship between the citizen and the State, including that it could undermine trust in the State[112]. In Norris's view, in giving evidence to that Committee, mass surveillance doesn't just undermine trust in the State, but "*promotes the view … that everybody is untrustworthy. If we are*

[108] Select Committee on the Constitution, HL Paper 18-II, 2009, p.31, q64
[109] Foucault, 1991, p.202
[110] Foucault, 1991, p.203
[111] Foucault, 1991, p.206
[112] Select Committee on the Constitution, HL Paper 18-I, 2009, paras 108-109

gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted"[113]. It should be remembered that Bentham's original panopticon was conceived of as a liberal reforming institution, in which those subject to its control had already been convicted of a crime and were to be made up as better citizens. In the digital panopticon, the trust that may be thought to exist between the State and its citizens is replaced with undue suspicion between the State and the citizen cast as a potential criminal, undermining the presumption of innocence.

Some argue that surveillance of this nature threatens to overturn the presumption of innocence, the fundamental norm upon which criminal justice in a democratic society is based – the "*golden thread*"[114] that runs through criminal law. While Weigand[115] says that there is only one presumption of innocence, that which exists after a criminal charge, there are competing strands of thought on what the presumption of innocence entails. Hadjimatheou observes that the presumption of innocence goes beyond a narrow procedural guarantee and that, in actuality, as it is understood in wider society it includes "*a right not to be treated as criminally suspicious unless one has done something to warrant such suspicion*"[116]. She refers to this as a 'wrongful criminalisation' view of the presumption of innocence[117]. An alternative view is what Duff calls 'civic trust'[118], involving a link between trust and the presumption of innocence in which the citizen should be trusted by the State to not be a criminal, which is supported by Milaj and Bonnici[119] and reflects Norris's view. The presumption of innocence in this sense is both a legal presumption – the procedural guarantee – and a moral presumption based on trust.

What unites Hadjimatheou and Duff is that while they take quite different theoretical approaches they both ultimately focus on what the presumption of

[113] Select Committee on the Constitution, HL Paper 18-I, 2009, para. 107
[114] *Woolmington v DPP* [1935] UKHL 1
[115] Wiegand, 2013
[116] Hadjimatheou, 2013, p.5; see also Nance, 1994; and Campbell, 2010
[117] Hadjimatheou, 2017
[118] Duff, 2013
[119] Milaj and Bonnici, 2014

innocence means in terms of what the State should not do – i.e. that it should not actively distrust citizens, for Duff's part, and that it should not wrongfully criminalise citizens, for Hadjimatheou's – rather than on the presumption as a strictly procedural guarantee. It is in this broader view of what the State should not do *vis a vis* the citizen, more fully reflecting the relationship between all individuals and the State, rather than just those who have been charged with an offence, that we should consider whether or not the digital panopticon undermines the presumption of innocence, as it is in this broader sense that the individual may understand their role within society, the nature of criminality, and their relationship with the State[120]. The key element in this broader sense of the presumption of innocence, which can be seen across both Hadjimatheou's and Duff's conceptions, is freedom from undue suspicion. A view of the presumption of innocence based on undue suspicion has received some tentative judicial support, with the European Court of Human Rights, while not going quite as far as either Hadjimatheou or Duff, agreeing in obiter that the retention of DNA samples of those who had been arrested on suspicion of a crime but not convicted contributed to a "*perception that they are not being treated as innocent"* in that *"their data are retained indefinitely in the same way as the data of convicted persons*"[121].

Compare this with the digital panopticon, where it is not just those who have been arrested but not convicted who have their data stored in the same way as those who have been convicted – it is everyone who participates in the digital world. Mass online surveillance, as the CJEU observed,

> *"affects all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings. It therefore applies even to persons for whom there is no evidence capable of suggesting that*

[120] Duff 2013
[121] *S and Marper v UK* [2008] ECHR 1581 at [122]

> *their conduct might have a link, even an indirect or remote one, with serious criminal offences"*[122]

The digital panopticon can be seen to extend the 'perception that they are not being treated as innocent', the undue suspicion, to include everyone who comes within its reach. Indeed, the Romanian Constitutional Court found that Romania's mass electronic surveillance regime

> *"equally addresses all the law subjects, regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to overturn the presumption of innocence and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes"*[123]

If we accept that the presumption of innocence is a broader principle than often assumed, encompassing the right to not be treated with undue suspicion, then it is clear that the digital panopticon does not sit easily with it. As Milaj and Bonnici put it, "*In the logic of mass surveillance programmes we can all potentially be involved in some criminal activities; we are all therefore general suspects*"[124].

Milaj and Bonnici further argue that even if the more narrow procedural conception of the presumption of innocence supported by Weigand is preferred then mass surveillance still erodes the effectiveness of that procedural guarantee. They say that the post-charge use of apparently irrefutable surveillance evidence gathered when the accused was not a suspect *de facto* overturns the burden of proof in criminal proceedings, placing the burden on the accused – who, due to the imbalance of knowledge between the individual

[122] *Watson* [2017] 2 WLR 1289 at [105]
[123] Romanian Constitutional Court Decision no 1258 from 8 October 2009
[124] Milaj and Bonnici, 2014, p.420

and the State inherent in surveillance, is unaware of the precise nature of what all the prosecution knows about their private life – to find some way to prove from the moment of arrest that the evidence to be presented by the State is not reliable[125]. Milaj and Bonnici's view is supported by Galetta, who says that the use of surveillance evidence in this way increases the 'innocence threshold' that must be overcome in order for the defendant to be acquitted[126]. And Edmond and San Roque show how lawyers, judges, and juries all tend to overestimate the reliability of surveillance evidence[127], with the result that evidence that is perhaps not entirely reliable may be assumed to be virtually irrefutable. With this assumption the burden of proof is further shifted onto the defendant and the 'innocence threshold' is raised even higher.

Galetta puts forward the idea that mass electronic surveillance is indicative of an ongoing shift from a 'post-crime' reactive model of policing, in which crimes are investigated and suspects prosecuted under a presumption of innocence, to a 'pre-crime' preventative model of policing, in which the police seek to predict crime through analysis of intelligence-derived data and then intervene at a preparatory stage before any crime actually occurs[128]. Maguire describes intelligence-led policing such as this as "*a strategic, future-oriented and targeted approach to crime control, focussing upon the identification, analysis and 'management' of persisting and developing 'problems' or 'risks' (which may be particular people, activities or areas), rather than on the reactive investigation and detection of individual crimes*"[129]. Van Brakel and de Hert say that characteristic of intelligence-led, surveillance-based, pre-crime policing is its insistence on building up intelligence through data collection[130], and the digital panopticon should be placed in this context. They argue that electronic surveillance allows the police to "*increase their fields of vision and to simultaneously collect evidence*"[131], and the mass retention of data at the heart of

[125] Milaj and Bonnici, 2014, p.425
[126] Galetta, 2013
[127] Edmond and San Roque, 2013
[128] Galetta, 2013; van Brakel and de Hert, 2011, p.166
[129] Maguire, 2000
[130] van Brakel and de Hert, 2011, p.168
[131] van Brakel and de Hert, 2011, p.171

the State's surveillance regime is in fact a mass retention of potential evidence that can be collated and analysed in order to predict crime or terrorism. In Galetta's view, in a predictive, pre-crime society everyone is a target of surveillance[132], and in the digital panopticon everyone, regardless of criminality, has their data gathered as potential evidence.

In this, rather than assuming that any given individual is innocent unless proven otherwise, everyone within the reach of the digital panopticon is initially assumed to be a potential criminal. Hadjimatheou argues that mass surveillance in fact helps the 'wrongful criminalisation' presumption of innocence as through the mass collection of what we can call potential evidence individuals can more readily be eliminated from criminal enquiries and wrongful convictions can be avoided[133]. But if anything this reinforces the point that, as Galetta puts it, "*everybody is considered as a potential offender in a pre-emptive society, regardless of the individual's [procedural] presumption of innocence, unless proved otherwise*"[134]. It is the fact of being considered to be a potential criminal in the first place that leads to potential evidence being gathered. Hadjimatheou, who bases her argument on CCTV surveillance, argues that the presumption of innocence cannot have been reversed by mass surveillance as if it was then it would look like a panopticon[135]. This is, in fact, as we have seen, what mass *online* surveillance looks like, even if CCTV does not. The emerging pre-crime policing enabled by mass online surveillance is therefore based on potential rather than actual criminality, potential rather than actual evidence, and pre-emptive rather than post-offending punishment[136]. Pre-crime policing enabled by mass online surveillance creates undue suspicion between the State and the citizen and stands contrary to the broader form of the presumption of innocence. If we presume that there are potentially criminals living in free society then we institute a regime whereby those for whom there is evidence of their involvement in serious criminality can be put under surveillance as an

[132] Galetta, 2013
[133] Hadjimatheou, 2017
[134] Galetta, 2013
[135] Hadjimatheou, 2017, p.45
[136] Galetta, 2013

exception to the rule. If we assume that everyone is a potential criminal then we put everyone under surveillance as the rule. The digital panopticon does the latter.

Norris contends that if the State is gathering potential evidence on citizens on the basis that they may commit future crimes then the State is changing the nature of the social contract[137]. Through the digital panopticon and its emerging pre-emptive practices that undermine the presumption of innocence and may at times reverse the burden of proof the role of the individual is fundamentally changed. Whereas in post-crime models only those for whom there is evidence that they have committed a crime should, in theory, come under suspicion and they continue to be presumed innocent until conviction, in the new pre-crime surveillance-based model, as Bauman et al observe, everyone is placed under an "*a priori suspicion that the individual then has to dismiss by his transparent behaviour*"[138]. In a mass surveillance society you are watched at all times so you need to at all times behave in such a way that the potential evidence being gathered at all times can't be used against you if in future you are accused of an offence. The digital panopticon remakes the digital citizen as a subject who is not just constantly visible but constantly under suspicion as a potential criminal who must moderate their behaviour in full view of the State. This is how panoptic uncertainty as a technology of power is utilised as a form of control, but in doing so it threatens to undermine the relationship between the citizen and the State and put everyone within the reach of the digital panopticon under an undue suspicion of potential criminality that can only by dismissed by their transparently acceptable behaviour.

4.2.2 | Undermining Freedom of Expression

Central to the panopticon is visibility; it is what gives rise to the imbalance of knowledge represented by panoptic uncertainty. True privacy cannot exist in a panopticon – privacy is invisibility, and with privacy the imbalance of visibility

[137] Select Committee on the Constitution, HL Paper 18-II, 2009, p.30, q56
[138] Bauman et al, 2014, p.122

that gives rise to the imbalance of knowledge which, in turn, gives rise to uncertainty cannot exist. Where the individual is visible in this way they may become less willing to engage in the exchange of ideas that are thought to be undesirable or potentially subversive. Freedom of expression does not just include the right to speak freely, but is also widely recognised to include the right to freely seek, receive and impart information[139] and, as such, is the keystone of a democratic society. While privacy and freedom of expression are often framed as competing interests in other contexts such as press regulation where a balance of rights may need to be struck between different persons, through the control mechanism of the digital panopticon they become tied together in the same person, now intrinsically linked. According to the UN's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "*Privacy and freedom of expression are interlinked and mutually dependent; an infringement upon one can be both the cause and consequence of an infringement upon the other*"[140]. As the Special Rapporteur finds, "*Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas*"[141]. And the potential impact of mass online surveillance has been recognised by the CJEU. In finding that bulk communications data retention is was incompatible with EU law, the Court opined that:

> *"Even if such legislation does not permit retention of the content of a communication … the retention of traffic and location data could nonetheless have an effect on the use of means of electronic communication and, consequently, on the exercise by the users thereof of their freedom of expression"*[142]

The interference with privacy required in the digital panopticon may lead to interference with the free exchange of ideas. Even when awareness of electronic

[139] See, for example, Universal Declaration of Human Rights art.19; Charter of Fundamental Rights of the European Union art.11; European Convention on Human Rights art.10
[140] United Nations Human Rights Council, 2013, para 79
[141] United Nations Human Rights Council, 2013, para 24
[142] *Watson* [2017] 2 WLR 1289 at [101]

surveillance extended only to what was understood before the Snowden leak the imbalance in visibility, knowledge, and power between the watched and the watcher that gives rise to panoptic uncertainty was present. But now that the true extent of this surveillance is public knowledge – and, as of 2015, 78% of Americans were aware of the NSA's programs[143] – the imbalance is even greater and the controlling effect on behaviour online has been empirically observed, as we shall now see.

Self-imposed restrictions on freedom of expression due to fear of State retribution are known as a 'chilling effects'[144]. Studies of internet user behaviour show how people change their behaviour in response to knowing about electronic surveillance in order to moderate their expression, demonstrating the effectiveness of panoptic uncertainty as a form of control. One study that compared search behaviour after the Snowden leak with search behaviour before the leak found that "*US-based search traffic falls by quite a large extent in the Google index for terms that are perceived as having an above average likelihood of getting you in trouble with the US government*" [145] and that there was "*empirical evidence that the surveillance revelations caused a substantial chilling effect relating to users' willingness to enter search terms that raters considered would get you into trouble with the US government*"[146].

Penney, in using Wikipedia page views as a measure of willingness to enter into an information exchange on 48 topics involving keywords that are used by the US Department of Homeland Security to monitor social media[147], found that after the Snowden revelations there was an "*immediate decline in traffic*"[148], with an average decline of just under 25% in the first month following the leak[149] across articles including those that are more obviously terrorism-related (including 'Al Qaeda', 'terrorism', 'suicide bomber', and 'Improvised Explosive

[143] Gao, 2015
[144] Hughes, 2012, p.399
[145] Mathews and Tucker, 2015
[146] Mathews and Tucker, 2015
[147] Penney, 2016, p.139
[148] Penney, 2016, p.117
[149] Penney, 2016, p.151

Device') and those that are perhaps somewhat less so (including 'political radicalism', 'extremism', 'fundamentalism' and 'nationalism'). Penney also found that an ongoing decline in traffic to these articles persisted long after the public became aware of the scale of surveillance, showing a strong upward trend in the 18 months prior to the revelations but still showing a strong downward trend 14 months later[150]. This suggests that knowledge of potentially being watched not only leads people to moderate their behaviour in the short term but also in the longer term and possibly even permanently[151]. Penney describes Wikipedia as "*an essential source of information and knowledge online, [functioning] as an important public tool to complement the democratic process in promoting collective understanding, decision-making, and deliberation*"[152], and points out that the activity involved – seeking out information on Wikipedia – is not only legal, but desirable in a healthy democratic society[153].

Further research by Penney has confirmed that the more that a given individual knows about online surveillance by SIAs the more likely it is that their speech is chilled[154]. He has also found that 62% of those studied said that they were somewhat less likely or much less likely to speak or write about certain topics online if they knew that they could be being watched[155], that 78% were somewhat or much more likely to think more carefully about what they say[156], that 78% were also somewhat or much more likely to think about what they search for online[157], and that 60% were somewhat or much less likely to post or share content on social media[158]. His research shows that young people and women are more likely than other groups to feel the chilling effects of mass online surveillance[159].

[150] Penney, 2016, p.151
[151] Penney, 2016, p.151
[152] Penney, 2016, p.125
[153] Penney, 2016, p.162
[154] Penney, 2017, p.12
[155] Penney, 2017, p.4
[156] Penney, 2017, pp.4-5
[157] Penney, 2017, pp.5-6
[158] Penney, 2017, pp.6-7
[159] Penney, 2017, pp.11-12

Noelle-Neumann introduced the idea of the 'spiral of silence' in the 1970s, in which, worried about isolation, people remain silent out of fear of society's reaction to their opinion[160]. Stoycheff shows that this takes effect in relation to online discussion and fear of prosecution resulting from State surveillance[161] and results in an empirically evidenced stifling of the expression of minority political views and the reinforcement of majority opinions[162]. As Wright says, "*People are scared when they learn about this. People stop accessing perfectly legal, legitimate and normal information because they are scared of those programs. That turns into a decreasing trend. The chilling effects … are real and empirically backed*"[163]. It is clear that the awareness of potential observation is enough to drive people to change their behaviour, and this must be seen as evidence of both the effectiveness of the digital panopticon as a technology of power in translating rationalities into reality and, as collectively we become more compliant, of capillary power in action.

The idea that a healthy democratic society is important for democratic government is one that is often acknowledged. As Balkin observes:

> *"democracy is about far more than a set of procedures for resolving disputes. It is a feature of social life and a form of social organisation … in which ordinary people gain a greater say over institutions and practices that shape them and their futures"*[164].

Balkin argues that what makes democracy is not just democratic *governance* but democratic *participation*, and that a democratic culture both extends beyond the institutions of democracy and underpins them[165]. According to Balkin, ICT changes the conditions of speech as it places freedom of expression in a new light, just as radio and television did in the past, greatly widening potential participation in the exchange of ideas but also creating new opportunities for

[160] Noelle-Neumann, 1974
[161] Stoycheff, 2016
[162] Stoycheff, 2016, p.308
[163] House of Commons Science and Technology Committee, HC 573-i, Q75
[164] Balkin, 2004, p.35
[165] Balkin, 2004, p.35

limiting and controlling that participation[166]. He argues that debates over freedom of expression should move from focusing on protecting only individual rights within a democratic process to focusing on protecting this wider democratic culture[167], writing that "*the free speech principle is about, and always has been about, the promotion and development of a democratic culture*"[168]. The chilling effect of the digital panopticon suggests that at the point at which potential democratic participation is widening, thus necessitating its protection in the name of healthy democracy, according to Balkin, there is in fact a reduction in the willingness of people to engage in discussion of certain topics.

The digital panopticon thus results in a significant chilling effect on the free speech of the digital citizen. In this, as is the case with the erosion of the presumption of innocence, the relationship between the digital citizen and the State is remade along new lines. Ideas that could be considered subversive, minority, or extreme may be pushed to the margins of public debate, reinforcing the existing order. As the digital citizen, who, through the erosion of the presumption of innocence, is cast as a potential criminal, becomes a passive subject of the control of the digital panopticon, their ability to engage in the free exchange of ideas that underpins democracy is undermined. In all, the digital citizen is rendered as a pliant, controllable entity, subject to the individualising power of the digital panopticon as the State seeks to extend its control.

4.3 | Maintaining Order

The rationality of the digital panopticon is rooted in security. What this means in practice depends on the nature of the society in which the governmentality is employed – in an authoritarian dictatorship, for example, 'security' may be directed towards the maintenance of the regime itself, in a liberal democracy it may be the security of the political institutions and the populace, and so on. A

[166] Balkin, 2004, p.3
[167] Balkin, 2004
[168] Balkin, 2004, p.28

technologically advanced form of the digital panopticon is used to help maintain the rule of the Communist Party in China, for example, and Russia has implemented a similar data retention framework as in IPA as the regime there seeks to cement its authority (which was found by the European Court of Human Rights to be incompatible with ECHR[169]). But the effect of the digital panopticon on the relationship between the digital citizen and the State in democratic societies calls into question its purpose. While it does not in law reverse the presumption of innocence or exclude the free exchange of ideas, and so on the face of it appears to be compatible with a democratic society, the reality of its nature is that, to some extent, it has the effect of doing those things. Bauman et al observe, in light of the Snowden revelations, that "*the old suspicion that agencies claiming to secure our life and wellbeing often turn out to be extremely dangerous retains considerable wisdom*"[170], and ask "*What, after all, are they supposed to be securing?*"[171]. If we wish to understand the rationality behind the digital panopticon as it has been employed as a governmentality in the US and the UK then we must consider the societal context in which it exists.

We should not assume that it is democracy, human rights, or the rule of law that is to be secured. The surveillance programmes undertaken by GCHQ and the NSA are of questionable legality and they undermine key principles of democratic society. The importance of this should not be overlooked, as it is the existence of a healthy democratic culture which fosters democratic norms among the population – including the presumption of innocence and the free exchange of ideas – that underpins the proper functioning of democracy. If this culture is undermined then democracy is undermined, with mass electronic surveillance leading, as Hintz and Brown found in their research into UK surveillance policy post-Snowden, to a power shift from citizens to the state[172] and, in the words of one of their interviewees, threatening a "*sustained degradation of democracy*"[173]. In the digital panopticon and in the name of

[169] *Roman Zakharov v Russia* [2008] ECHR 964
[170] Bauman et al, 2014, p.134
[171] Bauman et al, 2014, p.134
[172] Hintz and Brown, 2017, p.798
[173] Hintz and Brown, 2017, p.797

securing the democracy that it undermines the digital citizen takes on their new role as a potential criminal under constant suspicion, perhaps less willing to engage in an exchange of ideas that may be considered unpopular, undesirable, or subversive.

Bauman et al argue that "*it seems unwise to assume that these patterns* [of surveillance] *can be understood without some grasp on contemporary shifts toward globalizing markets and corporate wealth as the primary measure of economic and even political value*"[174]. According to Gill, the US is the "*military guarantor of disciplinary neo-liberalism*"[175]. In the post-Cold War era this role has been emphasised. As discussed in Chapter 2, disciplinary neo-liberalism seeks to 'lock-in' the power gains made by capital through the neo-liberal revolution[176], and Gill argues that it doesn't just use economic power to do so but also military power, including surveillance practices[177]. Harvey equally says that neo-liberal states in practice augment the coercive arm of the State with surveillance in order to protect corporate interests and, if necessary, repress dissent[178]. Haines, as the official historian of the CIA, argued that "*Following World War II the United States assumed, out of self-interest, responsibility for the welfare of the world capitalist system*"[179]. The NSA (as the US Government's principal global intelligence organisation, which focuses primarily on electronic surveillance and which has been described as the "*largest and most secret intelligence agency*"[180] and the "*inner circle of secrets*") and GCHQ (as the British Government's equivalent) should be seen as an extension of this military power. As Taylor Owen observes, "*The United States, which created the Internet as a defense research project, now considers cyberspace a 'domain' or potential battlefield equal in importance to land, sea, air, and outer space*"[181]. In the context of the western societies that have undergone a revolution informed by neo-

[174] Bauman et al, 2014, p.135
[175] Gill, 1995, p.3
[176] Gill, 2000, p.6; see Chapter 2.1.2
[177] Gill, 2008, p.206
[178] Harvey, 2005, p.77
[179] Chomsky, 1999, p.20
[180] Woodward, 1987, pp.46-47
[181] Owen, 2015, p.3

liberal social, political, and economic thought, the digital panopticon should thus be understood as a governmentality for maintaining the existing neo-liberal order.

This does not necessarily mean that SIAs themselves are motivated by a desire to secure neo-liberal order, specifically, out of some attachment to that particular order, only that they seek to ensure the security of the existing order, whatever that is, and which, in western societies, as we saw in Chapter 2, is fundamentally neo-liberal in nature. The digital panopticon moves towards a pre-crime, pre-emptive form of control, in which everyone is a potential criminal and potential threats to the order can be identified in advance and intervened upon. And in the digital panopticon the willingness of the digital citizen to seek out and impart information and ideas that may be considered to be subversive, extreme, or otherwise undesirable is diminished. We can thus understand that the digital panopticon exists to secure neither democracy nor the rule of law but as a governmentality to render the digital citizen governable according to security rationalities in order to maintain the contemporary disciplinary neo-liberal social, economic, and political order in which they play a part.

4.4 | Conclusion

The extent and global reach of GCHQ's and the NSA's online surveillance was revealed by Edward Snowden in 2013. With the advent of the internet and online forms of community and communication, where almost everything we do leaves a digital trace of some kind and all of our text messages, emails, telephone calls, internet searches, and online transactions (and more) are potentially observable, as well as advances in data collection, storage, and retrieval, and algorithmic analysis, surveillance now reaches deep into our lives in a way that would have been impossible just a decade ago. New forms of ICT facilitate both new forms of control and the extension of older forms of control to unprecedented and otherwise impossible degrees. It is inconceivable that

such an extensive, real time programme of global surveillance could have been undertaken in the pre-digital age.

Mass online surveillance has turned the UK into a digital panopticon, with serious implications for some of the most fundamental norms of a democratic society including the presumption of innocence and freedom of expression. In this, the relationship between the citizen and the State is remade by casting the digital citizen as a potential criminal deserving of constant observation who may, as a result, and particularly if they hold opinions that could be considered minority or subversive, feel unwilling to participate in the free exchange of ideas that is the keystone of democracy. And the digital panopticon should be understood as a governmentality that employs the technology of power of algorithmic panoptic uncertainty for translating security rationalities into reality so as to uphold the neo-liberal order in which the digital citizen plays a part.

So far we have seen how surveillance and big data techniques have been used by corporations and by the state to exert control over the digital citizen and render them governable according to the rationalities of surveillance capitalism and the digital panopticon. In the next chapter, we will see how the same techniques have affected democratic the public sphere through the surveillance of voters and microtargeting of political advertising to them, and how this facilitates the appropriation of the agency of the digital citizen as a political actor as they go about fulfilling the role of the choice-making active citizen engaged in consumer forms of online politics in the marketised public of the neo-liberal state.

Chapter 5 | The Algorithmic Manipulation of Online Public Space

In the previous chapters we saw how corporations have developed new technologies of power based around big data and the surveillance and modification of human behaviour, seeking to commodify as much of life as possible by translating the rationality of surveillance capitalism into reality. We have also seen how the State uses panoptic forms of online surveillance, with the co-operation of corporations like Facebook and Google and in part using the surveillance apparatus that they have constructed, to exert control over the digital citizen in pursuit of security rationalities. In this chapter we turn to politics and the public sphere, and will see how the architecture of surveillance capitalism, the surveillance-based governmentalities that corporations use to appropriate the agency of the neo-liberal digital citizen as a social and economic actor for their own ends, is also used to appropriate the agency of the digital citizen as a political actor for the ends of political forces.

Jürgen Habermas, sensing a decline in the public sphere and a crisis of democracy as a result of the domination of political discourse by the mass media, put forward the foremost account of the public sphere in 1967[1]. He argued that public spheres first emerged in the eighteenth-century coffee houses of England, *salons* of France, and *Tischgesellschaften* of Germany, and that, while they differed in many respects, they shared, at least in theory, a number of common elements[2]. For Habermas the public sphere is where "*society engaged in critical public debate*"[3] in which "*the authority of the better argument could assert itself against that of social hierarchy and in the end can carry the day*"[4]. He conceived of the public sphere as an uncoerced space created

[1] Habermas, 1989
[2] Habermas, 1989, pp.36-37
[3] Habermas, 1989, p.52
[4] Habermas, 1989, p.36

by critical public debate, the rational exchange of ideas between equals undertaken with the intention of reaching a consensus – the "*social space generated in communicative action*"[5]. Mark Poster characterise Habermas's view of the public sphere as being "*a domain of uncoerced conversation oriented toward a pragmatic accord*"[6]. The public sphere in Habermas's conception is not, then, simply a physical space that permits discussion, but the public social space created by that uncoerced discussion itself[7] (although, as Geiger notes, many analyses of the public sphere fail to recognise this distinction[8]). The concept of the public sphere is therefore vital in any discussion of the impact of the internet on the individual as a political actor, and freedom from coercion is at its heart. And the question of what impact online public spaces may have on the public sphere is one that has been addressed several times in the past by a variety of writers[9], but not for some time and thus not in relation to these spaces as they exist today, and not with the aim of identifying the surveillance-based forms of control to which the digital citizen is exposed to in those space and their impact on the digital citizen as a political actor.

So why is the internet, in particular, worth considering for its impact on the public sphere? Two reasons stand out. The first is that the internet provides for virtual public spaces to develop. While social media, discussion forums, and other online platforms are generally speaking privately owned and operated, they are usually public in that anyone can sign up and participate in discussion of ideas, sharing of posts and photos, and other interactions with other users (as Habermas put it, "*We call events and occasions 'public' when they are open to all, in contrast to closed or exclusive affairs*"[10]). The second reason is that since the internet's earliest days, writers have been highlighting its potential to increase access to information, give everyone a voice, and democratise debate. As Terje Rasmussen points out, "*What is genuinely novel with the Internet in a democratic*

[5] Habermas, 1996, p.360
[6] Poster, 1995
[7] Geiger, 2009, p.22
[8] Geiger, 2009, p.22
[9] See, for example, Dahlberg, 2001a; Dahlberg 2001b; Papacharissi, 2002; Dahlgren, 2005; Fuchs, 2014
[10] Habermas, 1989, p.1

perspective is that it cancelled the social division between speakers and listeners of the public sphere and made everyone into potential participants in numerous public interactions and debates"[11]. On this basis the internet is often lauded for its emancipatory potential, apparently promising to renew both the public sphere and democracy more generally and in the process to empower the citizen[12].

But there have also been concerns raised, not least by Habermas himself, about the internet's potential to increase the fragmentation of the public sphere[13] and about the domination of online public spaces by commercial interests through what we can recognise as surveillance capitalism, as was identified by Habermas in the age of mass media. Writing in 1993, in the earliest days of the influence of the World Wide Web, Howard Rheingold summed up this conflict: "*Virtual communities could help citizens revitalize democracy, or they could be luring us into an attractively packaged substitute for democratic discourse*"[14]. And the last few years have also seen an emerging and significant debate about the role of various forms of algorithmic manipulation of online public space in political processes across the world. The contribution of surveillance and big data techniques to this, and their impact on political campaigning and online discussion, should not be underestimated. As Renee DiResta says:

> *"We're heading down the path of an arms race in algorithmic manipulation, in which every company, political party, activist group, and candidate is going to feel compelled to leverage these strategies. We're at an inflection point … the marketplace of ideas is growing increasingly inefficient as unchecked manipulation influences our most important conversations."*[15]

[11] Rasmussen, 2014, p.1316
[12] See Geiger, 2009 for an overview
[13] Habermas, 2006, p.423
[14] Rheingold, 1993
[15] DiResta, 2017

Indeed, Nathaniel Persily, formerly the research director for the US Presidential Commission on Election Administration, questions whether democracy can survive the kind of disruption by algorithmic manipulation seen today[16].

Here we will discuss how the practices of surveillance capitalism have been repurposed to influence behaviour in the public sphere in order in order to try exert control over the digital citizen and appropriate their agency as a political actor through voter surveillance and the microtargeting of political advertising, and will discuss some of the ways that this impacts politics more generally. In doing so, we will identify the technologies of power to which the digital citizen as a political actor is subject to in online public spaces as well as the rationalities that underpin them, the effect that these have on online politics and on the digital citizen as a political actor, and the influence that they give political campaigns, corporations, and the State. While Habermas holds that the public sphere should be free of coercion – indeed, this is a key aspect of Habermas's idealised public sphere – some critiques build on Foucault's idea that no space is free of power to argue that it is impossible for public spaces to ever be free of some form of coercion[17]. This is where Habermas's concept of the public sphere meets our analysis of the new forms of control to which the digital citizen is exposed online, so we will locate voter surveillance and microtargeting both within the governmentality framework set out in Chapter 2, and in relation to the surveillance-based regimes discussed in Chapters 3 and 4, and will account for how these practices impact the digital citizen as a political actor exercising their agency as a sovereign consumer-citizen within the public sphere.

In all, the argument will be advanced that while the internet has been billed as a new, renewing, online part of the public sphere for all to come together, freely exchange ideas and information, and reinvigorate democracy, it is, in practice, severely lacking. We will see that in reality the neo-liberal digital citizenship of the internet of today enables new forms of control by political forces as they seek to manipulate democratic discussion and exercise greater influence over

[16] Persily, 2017
[17] See Villa, 2002

the political agency of the digital citizen. The online world, while allowing for public *spaces* to develop and facilitating political engagement and debate of sorts, thus fails to facilitate the development of an online and renewing part the public *sphere* in which digital citizens can receive and impart ideas free of coercion. Instead it continues the decline identified by Habermas in the 1960s. While the internet is now much more public and plays a much greater role in modern life than in the past, as a host for the public sphere it is deeply flawed.

5.1 | Voter Surveillance and Microtargeted Political Advertising

Recent years have seen the development of new techniques for online political advertising, where voters are surveilled by political campaigns in order to enable the microtargeting of precisely tailored advertising directly to them. Here we will see how the practices of surveillance capitalism are repurposed to facilitate this surveillance of voters and microtargeting of political advertising, thus bringing forms of coercion which have been developed to influence the behaviour of the digital citizen as a social and economic actor in pursuit of commercial desires into the public sphere in order to use them to influence the behaviour of the digital citizen as a political actor.

Targeting voters with advertising online isn't, of course, a new development. In 2001 Lincoln Dahlberg observed that *"Even democratically-oriented Internet sites are increasingly being hosted or directly run by corporate ventures promoting an individualized consumer-oriented politics that allows politicians to sell their messages directly to citizens online without the mediation of public discourse*"[18]. But in the past this was not done at the scale that can be reached today, or with the precision of targeting that can be achieved through the tracking of users and algorithmic analysis of massive datasets gathered through surveillance of the electorate. This allows political campaigns – whether they're

[18] Dahlberg, 2001a

candidates, parties, or referendum campaigns – to move beyond segmenting (a long-standing practice) to microtargeting individual voters and small groups who share desired characteristics. In the context of political campaigning this is known as 'microtargeting'. Zeynep Tufekci says that this kind of campaigning, which involves targeting individuals as individuals rather as members of broadly defined groups, has long been the "*holy grail*" of political campaigns[19], and argues that this kind of algorithmic microtargeting allows campaigns to attempt to 'engineer the public'[20]. Microtargeting has been described by Justin Hendrix and David Carroll as a nightmare for democracy[21]. Microtargeting may particularly be an issue in parliamentary systems such as the UK where governments are elected on the basis of electoral performance across a large number of small constituencies with plurality voting and where elections are often decided by a relatively small number of marginal constituencies[22].

As discussed in Chapter 3, predictive analytics – the informating through computer mediation of big data that lies at the heart of surveillance capitalism – allows for the discovery of otherwise unknowable information about people, rendering them hypervisible and knowable to an unprecedented degree[23]. The hypervisibility created by these techniques means that a wealth of personal information may be determined about an individual from relatively impersonal behavioural data. When this behavioural data is combined with personal data gathered by political campaigns and subject to the same techniques, campaigns can predict personality traits in individuals as well as the likelihood of individuals voting at all, of voting for their candidate, of being able to be persuaded to vote for their candidate, and of caring about particular issues or being susceptible to particular kinds of campaign messaging[24]. We will first look at some examples of microtargeting from recent political campaigns in the US and the UK before discussing this from a theoretical point of view, linking the practices of surveillance-based microtargeting with those of surveillance

[19] Tufekci, 2014
[20] Tufekci, 2014
[21] Hendrix and Carroll, 2017
[22] Bennett, 2013
[23] See Chapter 3 for a full exploration of how this operates
[24] Tufekci, 2012

capitalism and discussing how information (as potential knowledge) and power are connected as well as highlighting some of the effects of microtargeting on the political process. In all, we will recognise the practices of surveillance-based microtargeting as a co-option of the technologies of power of surveillance capitalism that should be understood as attempting to algorithmically manipulate the public and exert control over the digital citizen for political ends, which may give capital, foreign governments, and political organisations undue influence over the digital citizen and the democratic process

5.1.1 | Microtargeting in Practice

Campaigning that took advantage of big data techniques to engage with and target voters online was first seen at scale in the primary and Presidential election campaigns of Barack Obama in 2007 and 2008, and more extensively in his 2012 campaign[25]. In 2008, Obama was able to harness data gathering and analysis to engage with voters and embrace the social-movement-like nature of his grassroots[26], but it was in 2012, with dissipated enthusiasm among voters after four years of financial crisis and deadlock in Congress, that his campaign embraced big data behavioural modelling and analytics to engage in an unprecedented level of microtargeting in a handful of states in order to win a close election with carefully crafted, state-by-state tactics[27]. In the view of David Axelrod, Obama's chief strategist in 2008, the Obama's campaign's use of voter surveillance, behavioural modelling, and microtargeting in 2012 made 2008's campaign look prehistoric by comparison[28]. Microtargeting, for example, allowed the 2012 Obama campaign to reach inside specific voting districts that would otherwise vote Republican to pick out voters that they predicted would be sympathetic to their campaign's message and microtarget them with tailored advertising[29]. In doing so, they could avoid spending money on more generalised advertising across the whole district, which would likely have gone

[25] Bimber, 2014
[26] Bimber, 2014, p.131
[27] Bimber, 2014, p.131
[28] Johnson, 2012
[29] Tufekci, 2015

largely to waste, and instead spend it on microtargeting individual voters in order to attempt to improve their candidate's share of the vote on a state-wide basis (which, with the Electoral College system, is what matters).

A British company named Cambridge Analytica is thought to have taken microtargeting a step further than seen in Obama's campaigns in its work on Donald Trump's 2016 campaign, in that it merged behavioural data with personal data to create much more detailed data profiles of voters in order to produce psychometric profiles of voters based on this data (a process which it calls 'psychographing'). It is purported to have used data obtained from its work with the campaigns of Ted Cruz and Trump as well as personal and behavioural data obtained from data mining firms which it subjected to a form of predictive algorithmic analysis that it calls 'psychographics' in order to predict the psychological makeup of American voters and then microtarget them with ads tailored specifically for their psychological profile. It is believed that half of the Trump campaign's spending was on digital advertising, largely of this kind[30]. While doubts have been raised about the effectiveness of psychographing[31], Facebook itself is known to have mined users' emotional states and sold that information to advertisers[32]. Cambridge Analytica claims to have had 5,000 data points on over 230 million voters[33] allowing them to build target audiences and use this to engage voters and influence their behaviour[34]. It's known that Cambridge Analytica offered people small amounts of money in exchange for completing a survey, and that they also required them to download an app that would harvest personal and behavioural data both from their own Facebook profiles and from those of their friends[35]. However, it appears that much of the voter data used to microtarget voters ultimately came from other sources, including the Republican Party's own data operation[36].

[30] Persily, 2017, p.64
[31] Confessore and Hakim, 2017
[32] Levin, 2017
[33] Cambridge Analytica
[34] Cambridge Analytica
[35] Davies, 2015; Schwarz, 2017
[36] Confessore and Hakim, 2017

Research has shown the effectiveness of microtargeted political messaging online. A 2012 US study, carried out by Facebook, aimed at testing the effectiveness of online vote mobilisation operations, which compared targeted messages to official voting records released after polling day, found that these messages not only directly influenced the real-world voting behaviour of millions of people, but also influenced the friends of those people as well as friends of their friends[37]. While the difference was found to be small – with those who saw the message being 0.39% more likely to vote, and friends of those who saw the message being 0.11% more likely to say that they had voted[38] – across the large audiences that can be targeted on social media this could make a significant difference to the outcome of close elections in which every vote counts. The authors estimated that around 340,000 extra votes were cast in the 2010 midterm elections (out of a total of around 82 million) as a result of a single message placed by them on Facebook[39] (they note that in 2000 George W Bush effectively won the US Presidency as the result of a 537-vote margin in Florida, or less than 0.01% of all votes cast[40]). Facebook repeated the experiment for the 2012 Presidential election and again found a significant increase in voting as a result[41]. If such techniques are taken up by political campaigns seeking to turn out sympathetic voters who may otherwise not vote then the effect on the turnout of a campaign's supporters could be significant. Costas Panagopoulos argues that the ability to use microtargeting to mobilise a campaign's base in this way may even be a more effective route to electoral success than using it to attempt to persuade undecided voters[42]. Indeed, the 2012 Obama campaign (whose chief data scientist was previously employed in maximising the effectiveness of supermarket ad campaigns[43]) is known to have used similar techniques to successfully target people that they believed would be likely to support their candidate but who had a low likelihood of actually voting, leading one Romney aide to say that Obama had turned out voters that

[37] Bond et al, 2012, p.295
[38] Bond et al, 2012, p.296
[39] Bond et al, 2012, p.297
[40] Bond et al, 2012, p.295
[41] Jones et al, 2017
[42] Panagopoulos, 2015
[43] Tufekci, 2012

their campaign didn't even know existed[44]. However, Ballard, Hillygus, and Konitzer report that only 18% of ads in the 2012 Presidential election were 'get out the vote' ads, with the remainder being those soliciting donations or seeking to persuade or recruit potential voters outside the campaign's core vote by microtargeting them with adverts tailored to specific issues on which the campaigns predicted that they may be persuadable[45]. Some 67% of Obama's ads and 51% of Romney's ads appeared to be targeted at non-supporters[46].

In 2016 Cambridge Analytica launched 4,000 different ad campaigns and received 1.4 billion impressions (that is, its ads were viewed 1.4 billion times) in order to microtarget 13.5 million persuadable voters in sixteen battleground states, including the 'rust belt' states of the Midwest that proved crucial to Trump's victory[47]. The Trump campaign's own voter microtargeting operations, named Project Alamo, ran alongside Cambridge Analytica's and used data supplied by them[48]. According to the Republic Party's director of advertising, the Trump campaign ran 40-50,000 variations of its ads on any one day, with 175,000 variations on the day of the third Presidential debate[49]. In fact, some 31% of the Trump campaign's total expenditure was on online advertising, compared to 6% of Clinton's (and 9% for Obama in 2012)[50]. Part of their strategy was to target likely Clinton voters to try to dissuade them from voting[51], an inversion of the 'get out the vote' operations of Obama and Clinton. Nicole Rustin-Paschal observed in 2011 that microtargeting could potentially be used to provide information or disinformation designed to discourage susceptible potential voters from actually voting[52]. She argues that suppression operations, such as Trump's microtargeting-based campaign, intimidate voters out of exercising their right to vote by undermining their confidence in the

[44] Tufekci, 2012
[45] Ballard et al, 2016, p.416
[46] Ballard et al, 2016, p.417
[47] Persily, 2017, p.65
[48] Halpern, 08/06/2017
[49] Lapowski, 2016
[50] Williams and Gulati, 2017, p.7
[51] Persily, 2017, pp.65-66
[52] Rustin-Paschal, 2011

electoral process[53]. In 2016, Trump's team acknowledged that it was running three different opposition voter suppression operations in this way – targeting information about Bill Clinton's sexual history to young women, information about Hillary Clinton's 1994 comments on 'super predators' to African-Americans, and information about her support for the Trans-Pacific Partnership to idealistic young liberals who had supported Bernie Sanders in the Democratic primary[54]. These took advantage of Facebook's dark posts – or what it calls 'unpublished page posts'[55] – that allow page admins to deliver ads through audience filters, providing non-public ads to selected groups of users[56]. As a result of the effectiveness of these operations, the Trump campaign's digital director said after the election that "*Facebook and Twitter were the reason we won this thing*"[57].

As well as dark posts, which allow the microtargeting of narrow segments of users, Facebook provides a set of tools, known as 'Custom Audiences', which enable advertisers, including political organisations, to deliver advertising to specific individuals. These allow campaigns to submit lists of specific voters that they wish to target to Facebook, which then matches the entries on those lists to the Facebook profiles of those voters, allows them to be algorithmically filtered according to desired characteristics determined through their profiles and the surveillance of their online behaviour, and facilitates the sending of tailored advertising directly to those specific individuals. Facebook also provides a tool for identifying 'Lookalike Audiences', which allows advertisers to identify other users, who are not on their targeting list but share characteristics with those who are, to target with the same advertising, potentially dramatically expanding its reach. As well as this, there is a 'Website Custom Audiences' tool, which allows advertisers to implant a tracking pixel on their website (known as a 'web beacon') in order to keep note of which Facebook users visit that website, filter them, and microtarget those voters as well. And Facebook itself boasts about the

[53] Rustin-Paschal, 2011, p.912
[54] Green and Issenberg, 2016
[55] Tambini et al, 2017, p.16
[56] Tambini et al, 2017, p.16
[57] Lapowski, 2016

success of using their Custom Audiences tools to target specific voters. It cites the experience of a candidate for re-election to the US Senate in the 2016 elections, Patrick Toomey, saying that his campaign "*used a made-for-Facebook, audience-specific content strategy to significantly shift voter intent and increase favorability … contributing to his re-election*."[58]. Facebook claims a 10.5 point increase in pro-Toomey voter intention when using Custom Audiences (as well as a 19.4 point increase in voter intention among women aged 45-54 and a 13.1 point increase among men aged 55-64)[59]. These Custom Audience tools, including the Lookalike Audience tool, were also used extensively by the Trump campaign in 2016, allowing them to upload their voter lists, filter out undesired voters, and target the voters they wanted[60]. And at all times, whether using dark posts, Custom Audiences, or Lookalike Audiences, user engagement can be monitored, tracked, and analysed through the 'Conversion Tracking' tool so as to identify which ads are most effective with which demographic and more precisely hone the message.

Surveillance-based microtargeting appears to have taken place during the 2015 and 2017 UK general elections as well as the 2016 referendum on the UK's membership of the EU. While smaller parties with fewer resources may be largely limited to the use of spreadsheets and other relatively simple methods of data analysis[61], in 2015 the Conservative Party hired Obama's 2012 campaign manager Jim Messina and spent around 30% of their campaign budget on acquiring data, analytical behavioural modelling, and microtargeting undecided voters with specific concerns and behavioural traits[62]. However, much of their targeting came through phone calls and door knocks in marginal constituencies. They did, though, use online microtargeting, including Facebook's Custom Audiences, Lookalike Audiences, and Conversion Tracking[63] – according to Facebook's own account of how the Conservatives used their platform to microtarget voters, "*Using Facebook's targeting tools, the [Conservative] party*

[58] Facebook Business, *Success Story: Toomey for Senate*
[59] Facebook Business, *Success Story: Toomey for Senate*
[60] Halpern, 08/06/2017
[61] Anstead, 2017
[62] Chadwick and Stromer-Galley, 2016, pp.284-285
[63] Facebook Business, *Success Story: The Conservative Party*

was able to reach 80.65% of Facebook users in the key marginal seats. The party's videos were viewed 3.5 million times, while 86.9% of all ads served had social context – the all-important endorsement by a friend"[64]. The effectiveness of the tools used provided by Facebook led the Digital Director at the Conservative Party to say that "*for the first time in a UK election … digital made a demonstrable difference to the final election result*"[65]. During the 2016 Brexit referendum, the Vote Leave campaign, according to its director, Dominic Cummings, put around 98% of their money into digital, and served up about one billion microtargeted digital adverts during the official 10 week campaign, mostly via Facebook[66]. Thomas Borwick, Vote Leave's chief technical officer, says that "*We made full use of online marketing to ruthlessly target likely supporters online using innovative new ways to gain voter data*"[67]. They held most of their advertising back until towards the end of the campaign, when they were able to spend their money on the microtargeted adverts that surveillance-driven experiments earlier in the campaign had shown would be most effective[68]. As Cummings puts it, "*When things are digital you can be more empirical and control the timing*"[69]. In 2017, microtargeting was widely used by the major parties during the general election campaign. Voter surveillance and microtargeting has been identified as a key aspect in the Labour Party's campaign, helping them to close the sizable polling gap that existed before the election and bring about a hung Parliament[70]. According to Andrew Gwynne, then Labour's Elections and Campaign Chair, "*We put unprecedented levels of funding into online advertising, supported by a highly professional data targeting operation that gave us an edge in getting the right messages in front of the right voters. This allowed us to make quick decisions about who and where to target*"[71].

[64] Facebook Business, *Success Story: The Conservative Party*
[65] Facebook Business, *Success Story: The Conservative Party*
[66] Cummings, 2016
[67] Borwick
[68] Cummings, 2016; Cummings, 2017
[69] Cummings, 2017
[70] Gwynne, 2017
[71] Gwynne, 2017

It's worth noting that it isn't just through microtargeted advertising on social media platforms that political campaigns can use surveillance techniques to influence voter behaviour. Dan Siroker, director of analytics for Obama's 2008 campaign, tells us how the campaign in its early days tested several variations of its website in order to find the layout and wording which would be most effective in driving sign-ups to campaign emails[72]. By recording the behavioural responses of visitors, they were able to determine which combination was most effective, and increase the rate at which voters provided personal information to the campaign. Siroker estimates that in doing so they were able to persuade almost three million more people to sign up. As each sign-up ended up donating an average of around $20 to the campaign, this single experiment – based on surveillance of user behaviour and big data analysis and similar to the hypernudging performed by websites such as Facebook – is estimated to have provided them with around $60m of extra campaign funding. Campaigns can use their own data and their own analysis to target voters in many locations, particularly in attempting to drive fundraising, but Facebook is now arguably the most effective way to microtarget voters[73].

All of the microtargeting operations discussed here are examples of political campaigns employing the technology of power of algorithmic governmentality – involving voter surveillance, predictive algorithmic analysis, and microtargeted advertising – in order to create a contact point where the behaviour of the voter can be directed in the way desired. We will move on now to discuss what this means in terms of information, knowledge, and power, and will locate voter surveillance and microtargeting within our governmentality framework as repurposing the technology of power of algorithmic governmentality for political purposes.

[72] Siroker, 2010
[73] Anstead, 2017

5.2 | Information, Knowledge, and Political Power

Just as surveillance capitalism datafies the digital citizen and microtargets them based on those datafied representations of their physical selves, their data doubles, so too surveillance-based microtargeting involves creating datafied doubles of individuals and microtargeting them on this basis. Much of the work in this is done by the surveillance capitalist corporations themselves – it is often them that gathers much of the behavioural data used in microtargeting through dataveillance, and it is often through their platforms that the desired individuals can be identified and microtargeted with online political advertising (and, of course, these corporations financially benefit from microtargeted political ads placed on their platforms). Here we will address some of the issues that this raises in terms of informational asymmetries, and therefore power asymmetries, and in relation to a lack of transparency and accountability and the influence of capital in the political process.

Surveillance-based microtargeting involves, in part, taking the behavioural surplus produced by the digital citizen's work as a produsumer in surveillance capitalism and using it to attempt to influence their behaviour as a political actor. This involves a form of the descending individuation described by Foucault, by which people are distinguished from one another and governed individually with reference to some idealised norm[74]. Through this process, as Kreiss points out, campaigns can develop narrow appeals to different groups of voters, "*appearing to be all things to all people*"[75]. Doing so allows political campaigns to focus wedge issues on sympathetic voters without the risk of potentially motivating voters who strongly disagree with a party or a candidate's position[76]. This relies fundamentally on fragmenting the public and creating instead a multitude of different 'publics', each individually and algorithmically tailored to a particular individual. In fact, each of these 'publics' becomes less and less *public* and seen only by the individual, to the extent that

[74] Foucault,1980, p.39
[75] Kreiss, 2012
[76] Tufekci, 2014

in truth they may even be considered to be private. As Tufekci argues, this turns political communication into a highly personalised, private activity[77]. Individuals each become subject to exercises of power tailored to them, with the intent of making them up to that standard – in this case, that of a political actor exercising their agency in the manner desired by political campaigns. As such, not only do the practices of surveillance capitalism render the digital citizen amenable to new forms of control by corporations, but also to new forms of control by political forces.

As noted in Chapter 1, any given algorithm exists because somebody somewhere has a goal that they wish to attain through algorithmic computer mediation, whether that's ranking search results or delivering targeted advertising[78]. In this context, the goal (or rationality) to be translated into reality by the technology of power of surveillance capitalism, which seeks to influence consumer behaviour in order to produce that which is most profitable for corporations, that of the algorithmic governmentality identified by Antoinette Rouvroy, is political in nature, with campaigns seeking to influence the behaviour of the digital citizen in such a way as to benefit them. To do this, personal and behavioural data obtained from surveillance capitalism companies, and from other sources, is algorithmically analysed, and the resulting information is used to nudge voters with a view to influencing their political views and behaviour. In this, the practices of algorithmic governmentality are repurposed in order to seek to influence voter behaviour and so produce a change in (or a reinforcement of) a given voter's political view and thus the campaign's desired outcome either through donations, through spreading the campaign's message to friends or family, or in the voting booth. For example, using psychometric profiling campaigns could identify voters who are likely to become more conservative in their opinions when their fears are aroused and target them specifically with adverts designed to trigger that response – in relation to, say, crime, terrorism, family safety, or health – without showing those ads to people on whom they would have little to no (or even the

[77] Tufekci, 2014
[78] Chapter 3.1.2

opposite) effect[79]. As well as the individuation discussed already, microtargeting of this kind also breaks the individual themselves down into their component parts through the same process of dividuation as seen in surveillance capitalism. The digital citizen as a political actor becomes a collection of datafied parts, with each part to be addressed separately by those seeking to influence their behaviour and win their vote. The digital citizen ceases to be a whole and coherent individual and becomes instead a fragmented dividual, a composite[80] of "*multiple forces, identifications, affiliations, and associations*"[81]. As Tufekci says, if those seeking to influence voter behaviour in the twentieth century had "*magnifying glasses and baseball bats*", those of the twenty–first century have acquired "*telescopes, microscopes and scalpels in the shape of algorithms and analytics*"[82].

5.2.1 | Informational Asymmetries

As we have seen with surveillance capitalism, information is potential knowledge and power is maintained through the control of knowledge[83]. Key to exerting control over the digital citizen as a political actor is the informational asymmetry between campaigns and voters produced through surveillance-based microtargeting. As Howard and Kreiss argue,

> *"Asymmetries in information between political actors and voters, in turn, facilitate the ability of elites to manipulate the electorate. For example, candidates and their agents — paid operatives or citizen–supporters enlisted to spread their message and generate data on their friends and neighbors — know a lot more about those they are seeking to represent than citizens do about them. This makes these forms of 'personalized political communication' fundamentally transactional and manipulative, as campaigns and their supporters*

[79] Tufekci, 2014
[80] Isin and Ruppert, 2012, p.12
[81] Hintz et al, 2017, p.733
[82] Tufekci, 2014
[83] See Chapter 3.2.2

> *strive to tailor their political speech in terms of what individual voters want to hear"*[84]

As such, the ability to surveil voters and analyse the data obtained through that surveillance is, in fact, the ability to produce knowledge about those voters and extend power over them. This creates an unequal public, where some political campaigns know a lot about voters while voters know little about their microtargeting practices or how they operate (as a result of a number of factors, including algorithmic opacity, the fact that campaigns may wish to keep their microtargeting operations out of public view, and so on). Just as the practices of surveillance capitalism involve an appropriation of consumer sovereignty in part through the creation of informational asymmetries, so too surveillance-based microtargeting involves an appropriation of the political agency of the digital citizen through the creation of the same asymmetries. Political campaigns use the knowledge that they can generate about voters to subject them to manipulative microtargeted advertising, carefully crafted to trigger desired psychological responses, in an attempt to direct their agency in a manner that benefits the campaign, subjecting the digital citizen to new forms of control. Howard and Kreiss argue that surveillance of voters in this way, whereby they are rendered hypervisible and knowable to an unprecedented degree, has negative consequences for their willingness to engage in democratic debate and participation. In their view, privacy allows citizens to form their own viewpoints and develop political identities free from surveillance and public pressure, thus ensuring more robust political debate[85].

And just as asymmetries in information create asymmetries in potential knowledge and therefore asymmetries in power, so too controlling access to information means controlling access to potential knowledge and therefore confers power. In microtargeting on social media, surveillance capitalism corporations take up, according to Tambini et al, "*positions of great power gatekeepers of information, with the ability to facilitate or impede information*

[84] Howard and Kreiss, 2010
[85] Howard and Kreiss, 2010

dissemination"[86], but with few, if any, safeguards. Tufekci argues that "*By holding on to the valuable troves of big data, and by controlling of algorithms which determine visibility, sharing and flow of political information, the Internet's key sites and social platforms have emerged as inscrutable, but important, power brokers of networked politics*"[87]. Jonathan Zittrain warns of the potential for what he calls 'digital gerrymandering', or "*the selective presentation of information by an intermediary to meet its agenda rather than to serve its users*"[88]. Tufekci highlights the influence over elections that control of the flow of information in this way potentially gives social media platforms:

> *"A platform that wanted to manipulate election results could, for example, model voters who were more likely to support a candidate it preferred and then target a preponderance of such voters with a 'civic' message narrowcast so that most of the targets were in the desired target group, with just enough thrown in from other groups to make the targeting less obvious. Such a platform could help tilt an election without ever asking the voters whom they preferred (gleaning that information instead through modeling, which research shows is quite feasible) and without openly supporting any candidate. Such a program would be easy to implement, practically undetectable to observers (since each individual only sees a portion of the social media stream directed and nobody sees the totality of messages in the whole platform except the platform owners), easily deniable (since the algorithms that go into things like Facebook's news feed are proprietary and closely guarded secrets), and practically unconfirmable"*[89]

As Tambini et al argue, social media companies "*are in a position – should they wish – to offer different terms and services to different campaigns, and even to deny certain campaigns access. They could in theory make it easier for a political*

[86] Tambini et al, 2017
[87] Tufekci, 2014
[88] Zittrain, 2014
[89] Tufekci, 2014

party with which their business or ideological interests align to reach their supporters, or vice versa"[90]. Although there is no evidence that such digital gerrymandering has yet taken place it remains a possibility, and the willingness of these corporations to use their platforms to further their political goals is not hypothetical. For example, in 2012 Google ran a blacked-out version of its homepage 'doodle' (where they often replace the Google logo on their homepage with art, animations, or games) in protest against the proposed US Stop Online Piracy Act, which Google said would facilitate censorship, and provided a link to a blog post setting out its concerns[91]. Google's use of its website – the most visited site on the entire internet, with around 1.5 billion daily views as of 2012 – to advance a political view in this way passed largely without comment[92]. Digital gerrymandering may become a more pressing issue in light of persistent speculation over whether Facebook's founder and CEO, Mark Zuckerberg, intends to launch a campaign for the 2020 US Presidential election[93].

Microtargeting also produces informational asymmetries between political campaigns, as well as the asymmetry between campaigns and voters discussed already, potentially greatly amplifying the influence of capital in political campaigning. Smaller organisations with fewer resources cannot engage in this kind of surveillance-driven microtargeting. This manifests in three ways – first, that smaller organisations may not have the resources to collect large quantities of data; second, that they might not have the resources to subject the data that they do hold to the same degree of predictive algorithmic analysis that better-resourced organisations can perform; and third, that they may not have the resources to buy targeted advertising on online platforms to the same extent that better-resourced organisations can. Not only does this create an asymmetry in the quantity of data that can be gathered, but, as data provides information which in turn is potential knowledge, it also creates an asymmetry in the knowledge that political campaigns can potentially generate about voters from

[90] Tambini et al, 2017, p.13
[91] Google, 2012
[92] Zittrain, 2014
[93] Zittrain, 2014

that data and in the extent to which adverts can be microtargeted more individually to voters in key demographics or marginal constituencies.

This may dramatically increase the influence of money on political campaigning and thus confer a competitive advantage on those who can afford to obtain data, perform algorithmic analysis, and microtarget advertising. As Howard and Kreiss point out, if non-institutional and non-wealthy candidates of major parties are at a competitive disadvantage, those of other parties with fewer resources and comparatively little organisational infrastructure have access to few of the advantages available to institutional political actors[94]. An example can be found in the 2015 UK general election – while the Conservative Party was spending millions of pounds on voter surveillance, predictive analytics, and microtargeting across numerous marginal constituencies, the Green Party was limited to using Excel spreadsheets to assist them with campaigning in the constituencies in which their leaders were running[95]. Through this informational asymmetry, offline financial status and political status are translated into significant online status and influence, thus potentially greatly amplifying offline status and influence to the benefit of established or wealthy campaigns and disadvantaging others. This informational asymmetry therefore creates power asymmetries between those already involved in mainstream politics (such as established parties and candidates) and those outside of the political elite (such as new or smaller parties and candidates), reinforcing their difference in status in online spaces and increasing the influence of capital in the democratic process.

5.2.2 | Transparency and Accountability

As noted above, microtargeting lacks transparency and accountability and comes with the same issues with algorithmic opacity as is seen in surveillance capitalism. Not only can we not know the algorithms by which political campaigns segment and profile voters, but we can also not know the algorithms

[94] Howard and Kreiss, 2010
[95] Anstead, 2017

by which companies such as Facebook determine which voters meet the criteria set by those campaigns. Further, we generally speaking have thus far now been able to know which ads are shown to other people. In Tufekci's view, and unlike TV ad campaigns, online ads microtargeted at individuals "*take persuasion into a private, invisible realm*"[96]. As she points out, "*Misleading TV ads can be countered and fact-checked. A misleading message sent in just the kind of e-mail you will open or ad you will click on remains hidden from challenge by the other campaign or the media*"[97]. This is seen particularly in relation to Facebook's 'dark posts' which are targeted based on Facebook's audience filtering and remain invisible to users other than those specifically selected in line with the filtering criteria. In this kind of microtargeting there is little transparency or accountability either in relation to any false or factual claims made in those ads or in relation to the selection both of filtering criteria and of users who are predicted to meet those criteria. This lack of transparency and accountability also extends to the fact that Facebook generally doesn't disclose which organisations are spending what money on which ads.

This lack of transparency and accountability means that a range of actors beyond campaigns may be able to take advantage of the surveillance and microtargeting services offered by Facebook. Indeed, it is apparent that some of the microtargeting has taken place under the direction of foreign governments seeking to influence democratic votes. In September 2017 Facebook reported that targeted political advertising had been purchased by Russian entities during the 2016 Presidential election period and that it had passed evidence of this to the US special counsel investigating Russian interference in the election[98]. Facebook says that Russian entities masquerading as US users placed some 3,000 ads, focusing on divisive political and social issues, in 2015 and 2016 as they sought to influence the election[99]. In total, some 10 million people in the US are estimated by Facebook to have been exposed to Russian microtargeted advertising before and after the 2016 Presidential election, with

[96] Tufekci, 2012
[97] Tufekci, 2012
[98] Stamos, 2017
[99] Stamos, 2017

most adverts focusing on socially and politically divisive issues such as LGBT rights, race relations, and gun control[100]. In response, Facebook has indicated that it intends to end the practice of dark posts in relation to political advertising, and that it intends to increase transparency and accountability in a number of ways[101]. This includes by providing contextual information on which organisation paid for each ad, by allowing users to see other ads paid for by that organisation which are not targeted to them, and by requiring that companies wishing to place political advertising during US federal elections provide evidence that they are who they say they are.

Microtargeted advertising is one of several ways by which public space can be algorithmically manipulated for political ends, and has begun to be used extensively in political campaigning both in the US and the UK. This repurposes the technologies of power of surveillance capitalism, which exist to predict and influence human behaviour at scale and with ever-increasing accuracy, for political purposes, seeking to exercise control over the agency of the digital citizen as a political actor. In doing so, surveillance-based microtargeting creates informational asymmetries between voters and campaigns and between campaigns themselves, and thus imbalances in the possession of and potential access to knowledge, and amplifying the influence of capital in the electoral process. And the opaque and unaccountable nature of these practices has opened the way for foreign actors to exercise influence over democratic elections.

5.2.3 | Contextualising Microtargeting

What we see, then, with these voter surveillance and microtargeting practices is that the digital citizen in exercising their agency as a political actor – involved in liberal individualist and consumer forms of online political participation and acting out the process of perpetual engagement and choice-making in the marketised state, including the public sphere, in the pursuit of their own

[100] Schrage, 2017
[101] Kaplan, 2017

utilities as is expected of all sovereign citizens in neo-liberalism – is exposed to new forms of control by political organisations who make use of the apparatus and governmentality of surveillance capitalism for their own purposes in the online public sphere. The process of self-commodification – which, again, is expected of all citizens in neo-liberalism and which is taken advantage of by surveillance capitalism as it datafies and thus appropriates the commodified individual and sells them for profit – also allows the digital citizen to more easily datafied, filtered, and microtargeted in this context.

As discussed in Chapter 2, the consumer forms of politics seen online mean that the digital citizen must primarily exercise their agency as a political actor through active choice-making. Yet, as the sovereign individual of neo-liberalism, the digital citizen themselves is responsible for their failure to exercise that agency without succumbing to outside influence, despite the effectiveness of algorithmic governmentality, including the hypervisibility created by surveillance and algorithmic analysis and the power of hypernudges, in predicting and modifying human behaviour. These forms of control seek to leverage informational asymmetries so as to appropriate that agency, and thereby to influence the digital citizen to exercise that agency in such a way as to benefit the political organisations in question (whether through donating, through attempting to influence the opinions of others, or through voting). Similar informational asymmetries also disadvantage non-establishment and less resourced political parties, campaigns, and candidates, with the effect of increasing the influence and therefore the power of capital in the democratic process, thus reinforcing disciplinary neo-liberalism as it seeks to 'lock in' the power gains that capital has made in society more generally over the last few decades.

In this way, forms of coercive power which were developed in order to pursue the rationalities of surveillance capitalism by appropriating the agency of the neo-liberal digital citizen as a social and economic actor and directing it for commercial gain are repurposed by political parties and campaigns in order to appropriate their agency as a political actor and direct it for political gain.

However, and while it is indeed the case that the practices described herein represent a different application of the same targeting tools which were initially developed for use in a commercial context and which were discussed in Chapter 3, what is clear from the preceding discussion is that the effect of using these tools in a political context for microtargeting is specific and specifically detrimental to the political process and to the public sphere. The practices of voter surveillance and microtargeting therefore bring powerful coercive tools into the public sphere, moving it further away from the ideal put forward by Habermas.

5.3 | Conclusion

In this chapter we have identified the technologies of power based around surveillance and big data that the digital citizen encounters as a political actor in the online world, and seen some of the ways in which these new forms of control impact on the democratic process more generally. Far from providing for a new arena for a renewed public sphere of uncoerced discussion, what we have seen developing online are instead spaces where, in pursuit of certain agendas, voters are surveilled by political campaigns in order to enable the microtargeting of tailored advertising targeted directly to them so as to influence their behaviour as a political actor. As such, the public spaces that have developed on the internet cannot be considered to provide for an online renewal of the public sphere but instead to continue the decline identified by Habermas.

Here we have explored how voter surveillance and microtargeting by political campaigns and foreign influences takes advantage of services offered by sites like Facebook which have built powerful engines for predicting and modifying human behaviour in pursuit of the rationalities of surveillance capitalism. In this the digital citizen is subject to new dataveillance-based forms of control, in which the algorithmic governmentality of surveillance capitalism is repurposed for political ends. We have identified the ways in which this creates

informational asymmetries – and therefore knowledge and power asymmetries – between voters and campaigns as well as between campaigns themselves, thus potentially greatly increasing the influence of capital in the electoral process and reinforcing disciplinary neo-liberalism as it seeks to 'lock in' the power gains made by capital over the last few decades. In doing so we have seen how the governmentalities, rationalities, and technologies of power that operate in these online settings work to influence the political behaviour of the digital citizen. These involve surveillance, big data techniques, and algorithmic control for the purpose of appropriating the political agency of the digital citizen and exerting control over them as a political actor – taking advantage of features of neo-liberal digital citizenship, including the prominence of liberal individualist forms of online consumer politics and the need for perpetual choice-making in the marketised state, encompassing the public sphere, as well as the self-commodification that facilitates surveillance capitalism – and we can place these alongside the forms of control over them as an economic and social actor identified in previous chapters.

At the core of the concept of the idealised public sphere lies the principle that people should be able to come together freely, without coercion, to discuss ideas and exchange information. This is not the case online. The use of these technologies of power should be understood as attempts to algorithmically engineer the public in order to manipulate public space, and may give corporations, capital, and political organisations undue influence over the digital citizen and the democratic process. Online public spaces are not, therefore, sites of uncoerced debate. Instead they are spaces in which the digital citizen is subjected to powerful new forms of political influence and control, making them coercive spaces in which the technologies of power of algorithmic governmentality are utilised for political ends. Through these technologies, the way that the contemporary internet operates leaves the digital citizen in the neo-liberal mould open to new forms of political control, further empowering corporations, capital, and the political establishment at our expense and continuing the decline of the public sphere. And by locating the algorithmic manipulation of online public space in the context of the commercial

surveillance regimes discussed in Chapter 3 we can understand this to be the product of human choices made in the pursuit of rationalities in which public space becomes amenable to manipulation by political forces as well as commodification and control by corporations.

In the next chapter we will assess the challenges that the surveillance practices discussed in this thesis so far, including those in the public sphere, pose for data protection and privacy. We will also look at some of the reforms that have been proposed or are forthcoming, as well as the extent to which data protection and privacy law may allow the digital citizen, as a self-managing sovereign actor, to manage and thus protect their privacy and their data.

Chapter 6 | Privacy, Data Protection, and Online Surveillance

So far we have seen how dataveillance is employed by corporations that seek the commodification of life through surveillance capitalism, by the State as it seeks to pursue security concerns and uphold the existing neo-liberal order through the digital panopticon, and by political parties and campaigns who seek to maximise their vote and maintain their position through voter surveillance and microtargeting. We have set out the links between these practices to show how they overlap and complement each other, blurring the distinctions between corporate, State, and political power. And we have discussed how these practices remake the relationship between the digital citizen and the corporation, between the digital citizen and the State, and between the digital citizen and political organisations. In all, we've shown that digital citizenship in the neo-liberal mould opens the individual up to these new forms of surveillance-based control, which seek to appropriate or control the social, economic, and political agency of the digital citizen in pursuit of economic, security, and political rationalities. In this chapter, we will look at the restrictions imposed on these practices by privacy and data protection law, the rights and remedies available to digital citizens in those frameworks that allow them to challenge such practices, and the effectiveness of these laws in providing protections in the era of dataveillance.

Online privacy is often thought of as being a matter of protecting our personal information from being seen by other people, and it is often assumed that in behaving properly and not disclosing too much information to others our privacy can be protected. But in focusing on other people we overlook the fact that in surveillance capitalism there is and can be no such thing as true privacy. Hypervisibility is central to the business model that drives the biggest players in the technology sector, raising questions of privacy and control of personal data. And hypervisibility is also central to the effectiveness of the digital panopticon,

both through the transfer of data between surveillance capitalism corporations and the security and intelligence agencies and through the State's own data collection and analysis practices. Foucault wrote that "*visibility is a trap*"[1], allowing the individual to be known and controlled, and while protections for privacy potentially offer an escape from this trap it should not be expected that these corporations will give up the significant profits that they can make through dataveillance easily, or that the State will willingly give up its ability to conduct mass surveillance. Indeed, when Hal Varian predicts that "*By 2025, the current debate about privacy will seem quaint and old-fashioned ... Everyone will expect to be tracked and monitored, since the advantages, in terms of convenience, safety, and services, will be so great*" [2] this should be taken as a statement of intent.

We will first address the issues raised by dataveillance in the context of surveillance capitalism, discussing how the prevailing 'notice and consent' model of data protection has been rendered inadequate by big data and predictive analytics, and will look at whether forthcoming reforms to data protection law, including the EU's General Data Protection Regulation[3] ('GDPR'), can adequately address these issues. We will then assess the extent to which the voter surveillance and microtargeting practices described in Chapter 5 will be permissible under GDPR and the EU's proposed ePrivacy Regulation[4], identifying the restrictions that will apply to such activities under that legislation, the obligations placed on political organisations that wish to microtarget voters, and the tools provided in law for voters to resist these practices. Finally, we will examine the compatibility of the British Government's communications data retention and disclosure powers under the Investigatory

[1] Foucault, 1991
[2] Raine and Anderson, 2014
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 ('GDPR')
[4] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ('Draft ePrivacy Regulation')

Powers Act with the ePrivacy Directive[5] in light of recent decisions of the CJEU. These provisions, commonly known as the 'snooper's charter', appear to be incompatible with the Directive on a number of grounds.

In all, this chapter will show that pervasive dataveillance poses serious challenges for privacy and data protection law and that further reforms may be needed, but also that these laws do provide ways to restrict and to challenge surveillance practices and do provide some tools which may be of use to the digital citizen as they self-manage their privacy and seek to resist control.

6.1 | Privacy and Data Protection in Surveillance Capitalism

There are real challenges for privacy and data protection in surveillance capitalism, and new approaches may be needed. We will set out some of these issues and discuss some of the developing legal responses, including GDPR and the proposed ePrivacy Regulation, seeking to determine whether they will provide effective protections for the digital citizen.

6.1.1 | Challenging Existing Protections

The current approach to privacy and data protection is inadequate. Current and planned data protection legislation – such as the Data Protection Act 1998 ('DPA'), as well as forthcoming legislation like GDPR and the Data Protection Bill – is fundamentally built around a 'notice and consent' model. This relies on what Solove calls 'privacy self-management'[6], which he says "*takes refuge in consent*"[7]. But when data about every aspect of life is gathered on a vast scale, when predictive algorithmic analysis can potentially disclose a significant amount of

[5] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 ('ePrivacy Directive')
[6] Solove, 2013
[7] Solove, 2013, p.1880

private, otherwise unknown information, and when it is in the interests of surveillance capitalism corporations to minimise the likelihood of users protecting their privacy then whether adequate notice, let alone adequate consent, can truly be given comes into question[8].

Facebook serves as a typical example of how dataveillance techniques challenge existing models. Its data policy is relatively clear about the fact that it uses user data to personalise the service that it provides:

> *"We are able to deliver our Services, personalize content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things you're connected to and interested in on and off our Services"*[9]

But it also talks extensively of 'sharing' user data with partners with little indication that this actually means *selling* access to data to third party advertisers for profit. Facebook says that in sharing user data it "*work[s] with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world*"[10], but it gives no indication of who these third parties are or what they might do with the data.

While Facebook assures its users that none of the data that it shares with third parties contains personally identifiable information (the example that it gives of what might be shared is "*25 year old female, in Madrid, who likes software engineering*"[11]), we now know that even apparently anonymous data can be used to pinpoint an individual with a high degree of accuracy. In 2008, researchers were able to analyse an anonymised dataset of 500,000 Netflix subscribers and in doing so re-identified the profiles of known individuals, revealing their apparent political preferences and other potentially sensitive

[8] See, e.g. Solove, 2013; Hull, 2015
[9] Facebook, 2016
[10] Facebook, 2016
[11] Facebook, 2016

information[12]. They found that someone who knows only a little about a given Netflix user was able to re-identify that user's profile in the dataset[13]. Likewise, Sweeney demonstrated that, even with all other information discarded, 87% of Americans can be re-identified with a combination of just their zip code, gender, and date of birth, and that 53% of Americans can be re-identified with the less specific combination of their location more generally, gender, and date of birth[14]. And when New York City publicly released anonymised data about its licenced taxi drivers and the trips they had taken it took less than two hours for all 173 million entries to be completely de-anonymised and individuals re-identified[15]. Through analysis of publicly-available paparazzi photos of celebrities getting in and out of taxis it was determined which celebrities had taken which taxis from and to where, how much they had paid, and, in some cases, how much they had tipped[16]. And in 2017 researchers demonstrated that web browsing data can be easily de-anonymised and individuals re-identified and linked with their social media profiles with a high degree of accuracy[17]. Given Facebook's example of the information that it may share, the question must be asked of how many 25 year old female software engineers there actually are in Madrid. Each piece of information about an individual narrows the range of who it could be, regardless of whether a name or date of birth is included, so it is questionable whether apparently anonymised information such as this can ever be truly anonymous.

Beyond this, Crawford and Schultz talk about 'predictive privacy harms'[18], where poorly executed analysis creates harm by inferring or predicting inaccurate information that impacts on an individual's life[19]. This may particularly be an issue given the potential for algorithmic bias. But even where profiles are accurate there is potential for predictive privacy harm if they are

[12] Narayanan and Shmatikov, 2008, p.1
[13] Narayanan and Shmatikov, 2008, p.1
[14] Sweeney, 2000
[15] Goodin, 2014
[16] Trotter, 2014
[17] Su et al, 2017; see also Hern, 01/08/2017
[18] Crawford and Schultz, 2014
[19] Crawford and Schultz, 2014, p.93

not used appropriately – an oft-cited real world example is of a pregnant teenage girl whose father, who was unaware of her pregnancy, was alerted when the US supermarket Target, which had determined that she was probably pregnant through predictive analysis of changes in her shopping habits, sent her vouchers for products that pregnant women and new mothers may need[20]. As the girl hadn't told Target that she was pregnant this involves not just the unauthorised disclosure of personal information by Target, but also the discovery and unauthorised disclosure of this information by and to Target themselves in the first place as well as the exploitation of this information for corporate ends. And Facebook's 'people you may know' feature, which suggests potential 'friends' to connect with on Facebook, has in the past suggested not just users' therapists, but also other patients of their therapists[21]. Similar issues have been highlighted when it comes to sex workers, who may prefer to use a pseudonym when dealing with clients, with Facebook revealing their private identities to clients and raising very real safety concerns[22]. Facebook is also known to create a 'shadow' profile of information that users have never disclosed to it but which it has been able to obtain about them from other sources, such as other people's contact lists and phone books, which it uses to suggest friends and make other 'suggestions'. It has even in the past admitting to experimenting with using mobile phone location data to determine which people may know each other based on geographical proximity[23]. Given the potential for predictive privacy harms, it is questionable whether even users who read privacy notices have an informed understanding of the extent to which the data they are giving up may be used to reveal private information about them. And the potential for predictive privacy harms, as well as the potential for harm caused by re-identification or unauthorised disclosure of data, may be taken to extremes by the internet of things. IoT devices could gather significant amounts of data about individuals in the real world, potentially far beyond that obtained through the surveilling of behavioural data online. This may reveal much about an individual, and the potential for harm

[20] Duhigg, 2012
[21] Tait, 2016
[22] Hill, 2017
[23] Conger, 28/06/2016

either through re-identification or through predictive analytics could be greatly amplified.

As well as these issues, privacy notices themselves are often deeply problematic. They are often long and complex – one study estimates that it would take 244 hours each year to read every privacy notice seen by the average digital citizen[24] – and often obfuscate with euphemisms and legalese[25]. Solove observes that studies have repeatedly shown that most people neither read nor understand privacy notices[26] and concludes that, in any case, given the nature of dataveillance and the extent to which it occurs across many different platforms, "*even well-informed and rational individuals cannot appropriately self-manage their privacy*"[27]. Acquisti et al, in their review of the literature on this topic[28], find that there is considerable uncertainty on the part of users as to the consequences of giving consent to data sharing, and that their choice to consent or not is heavily dependent on contextual clues provided by the websites themselves. Yeung argues that "*the primary business model through which Big Data is being monetised preys directly upon the susceptibility of individuals' privacy behaviour to subconscious external influence, particularly the powerful heuristics associated with ostensibly 'free' services*"[29]. As a result of this, and of the issues highlighted above, Yeung goes as far as to call privacy notices in the context of dataveillance deceptive[30]. As Cate and Mayer-Schönberger point out, the challenges posed by big data to the notice and consent can "*leave individuals' privacy badly exposed, as individuals are forced to make overly complex decisions based on limited information, while data processors can perhaps too easily point to the formality of notice and consent and thereby abrogate much of their responsibility*"[31].

[24] McDonald and Cranor, 2008
[25] Turow, 2008, p.62
[26] Solove, 2013, pp.1884-1885
[27] Solove, 2013, p.1881
[28] Acquisti et al, 2015, 509–514
[29] Yeung, 2017, p.126
[30] Yeung, 2017, p.127
[31] Cate and Mayer-Schönberger, 2013, p.68

What is clear, then, is that the current model of notice and consent provides inadequate protections for the digital citizen. Big data practices in the context of surveillance capitalism expose significant flaws in this model of protection, and raise important questions. How can adequate notice be given when it is impossible to say what predictive analysis might reveal about an individual? How can an individual give informed consent when they can't reasonably be expected to understand what they're consenting to? The digital citizen is expected to protect their privacy and their personal data within a framework that is wholly inadequate for that purpose. Yet, as we saw in Chapter 2[32], neo-liberalism, in imbuing the individual with personal responsibility for all aspects of their life, places responsibility for failing to fulfil their role as the active, informed, self-managing citizen, regardless of informational, educational, or structural factors that lie beyond their control. And one of the central themes of self-management in neo-liberal digital citizenship is management of the digital self, including privacy self-management. In line with this, relying on notice and consent despite its inadequacies places responsibility for privacy protection – and therefore responsibility for failures to adequately protect privacy resulting in privacy violations – firmly with the individual. Indeed, Fuchs goes as far as to call research into this 'victimisation research'[33], such is the extent that the individual is held responsible for privacy violations that, in truth, may be beyond their control.

Approaches which can be more effective in the contemporary digital society are therefore sorely needed if we are to move beyond a model of protection which victimises digital citizens for failures beyond their control. As such, we turn now to discuss some of the ways that some of the issues with notice and consent are being addressed.

[32] Chapter 2.3
[33] Fuchs, 2011, p.146

6.1.2 | Protecting Privacy

Recognising that existing data protection frameworks are outdated and potentially ineffective in the modern world, the EU introduced GDPR to update and reform the legal regime. Coming into force until May 2018, it attempts to resolve some of the issues with notice and consent and forms the basis for other proposed reforms to privacy and data protection frameworks such as the EU's ePrivacy Regulation and the UK's Data Protection Bill. It's notable that GDPR was an initiative driven forward by a German Green Party MEP, Jan Albrecht, a representative from perhaps the most privacy-conscious Member State (as a result of German experiences under secret police from the 1930s through to the 1980s) and of a political tradition that stands at odds with the neo-liberal ideology which has prevailed in many parts of the west over much of the last few decades. As noted in Chapter 2[34], while the general direction of reform over the last few decades in many western countries has been towards neo-liberalisation, not all reforms have been neo-liberal in nature and they have often departed from that general direction. The adoption of GDPR by the EU is perhaps an indication of the extent to which the trend towards national-level neo-liberal politics may not always translate to neo-liberal reform at a supranational-level, where law, policy, and regulation takes into consideration the viewpoints and priorities of representatives from a variety of countries with different political cultures.

GDPR sets out some limitations on the use of personal data which may on the face of it be relevant in terms of limiting the practices of surveillance capitalism. GDPR requires that personal data be processed only for "*specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*"[35] (a principle known as 'purpose limitation'). It also requires that only data that is adequate, relevant and limited to what is necessary for the purpose be processed[36] ('data minimisation'), and that

[34] Chapter 2.1.2
[35] GDPR, art.5(1)(b)
[36] GDPR, art.5(1)(c)

personal data be stored for no longer than is necessary for that purpose[37] ('storage limitation'). These principles may appear to pose a problem for surveillance capitalism – as Edwards and Veale point out, for example, in Amazon's business model data collected for sell books is repurposed to sell adverts for book buyers[38]. Surveillance capitalism corporations may also take issue with being unable to store personal data indefinitely, and as they seek to obtain as much data about individuals and their lives as possible they may process far more data than is necessary for the purpose being sought.

GDPR also codifies the 'right to be forgotten' first established in the *Google Spain* case[39]. This allows a data subject to request that a data controller delete their personal data in a number of circumstances, including, inter alia, where the personal data is no longer necessary for the purposes for which it was collected and where the data subject objects to its processing[40]. However, the European Commission's Article 29 Data Protection Working Party has issued guidance on the right to portability under GDPR which makes clear that information about an individual which has been inferred from data provided by that individual (such as that obtained through predictive analysis of behavioural data) does not 'belong' to the data subject[41] (although, as Edwards and Veale observe, this appears to conflict with *Google Spain*[42]). There therefore seems to be an ambiguity about the precise extent to which the right to be forgotten applies under GDPR.

And GDPR potentially expands the scope of data protection by expanding the definition of personal data. Whereas, for example, DPA applied to data relating to a person who may be identified from that data (or from that data and other information held by or likely to come into the possession of the controller)[43], GDPR extends the definition of personal data to cover "*any information relating*

[37] GDPR, art.5(1)(e)
[38] Edwards and Veale, 2017, p.11
[39] *Google Spain v Agencia Española de Protección de Datos (AEPD) and González* [2014] WLR(D) 202
[40] GDPR, art.17(1)
[41] Article 29 Data Protection Working Party, 2016, p.8
[42] Edwards and Veale, 2017, pp.35-36
[43] Data Protection Act 1998 ('DPA 1998'), s.1

to an identified or identifiable natural person", and further provides that "*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*"[44]. This means that personal data now explicitly includes online identifiers, 'pseudonymous' data (that is, data which has been anonymised but when combined with other data can be related to an identifiable person)[45], and a data profile of an individual which could be used to single them out[46]. A similarly extended definition of personal data is also included in the Data Protection Bill[47]. And the processing of personal data by a controller outside the EU but relating to profiling of behaviour which takes place inside the EU comes under GDPR's remit, particularly when such profiling is "*in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*"[48]. A profile consisting solely of anonymised behavioural data relating to an indirectly identifiable individual located in the EU, which does not itself directly identify an individual and so may not have formerly been considered to be personal data under DPA, for example, would now come within the scope of GDPR, and would do so regardless of whether the data processing took place inside the EU or not.

As well as extending the definition of personal data, GDPR expands the scope of 'special' categories of personal data that receive protections above and beyond those applicable to 'ordinary' personal data (data falling into one of these categories is called 'sensitive data' in GDPR[49] and 'sensitive personal data' in DPA[50]). Under GDPR, biometric data, ("*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique*

[44] GDPR, art.4(1)
[45] GDPR, art.4(5)
[46] GDPR, recital 26
[47] DPB, clause 2(2)-(3)
[48] GDPR, recital 24
[49] GDPR, recital 10
[50] DPA 1998, s.2

identification of that natural person, such as facial images or dactyloscopic data"[51]) and health data ("*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*"[52]) will be considered to be sensitive data – as will, inter alia, data revealing racial or ethnic origin, political opinions, and religious beliefs, or concerning sex life or sexual orientation – and its processing will in most cases require explicit consent from the data subject[53]. This includes the processing of sensitive data obtained directly from data subjects, but information falling into any special category which is inferred from ordinary personal data, rather than obtained directly, as in the example of the pregnant teenage shopper at Target, is also considered sensitive data[54], as is apparently ordinary personal data from which information falling into one of the special categories can be inferred[55].

Moving on, GDPR provides various grounds for the lawful processing of personal data. Two of these – that the data subject has consented to the processing[56] (requiring explicit consent for sensitive data[57]), and that the processing is in the legitimate interests of the controller (which is applicable only to ordinary personal data)[58] – may be of relevance to surveillance capitalism. We will deal with the legitimate interests ground first. This requires a balance between the legitimate interests of the data controller and the interests and rights of the data subject, so may not be invoked in all circumstances. And the Article 29 Working Party has said in the context of the Data Protection Directive, which precedes GDPR and provides for the same balancing test[59], that data controllers who "*monitor the on-line or off-line activities of their customers, combine vast amounts of data about them from*

[51] GDPR, art.4(14)
[52] GDPR, art.4(15)
[53] GDPR, art.9
[54] Edwards and Veale, 2017, p.14
[55] Article 29 Data Protection Working Party, 2011, p.6
[56] GDPR, art.6(a)
[57] GDPR, art.(9)(2)(a)
[58] GDPR, art.6(f)
[59] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 95/46/EC [1995] OJ L281/31 ('Data Protection Directive'), art7(2)

different sources that were initially collected in other contexts and for different purposes, and create - and, for example, with the intermediary of data brokers, also trade in - complex profiles of the customers' personalities and preferences" without their consent are likely to present a "*significant intrusion*" into the privacy of the data subject and the controller's legitimate interest would be overridden by the interest and rights of the data subject[60]. So it would seem that the legitimate interest ground for processing ordinary personal data is unlikely to be available to corporations engaged in the practices of surveillance capitalism. This leaves consent as the only ground which potentially can apply.

GDPR deals with some of the issues with notice and consent directly. It provides that notice must be "*presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language*". Notice which does not meet these requirements will be not be binding[61]. GDPR also says that in assessing whether consent is freely given, utmost account shall be taken of whether the provision of a service is conditional on consent to the processing of personal data that isn't necessary for the provision of that service[62]. This potentially mitigates to some extent the problem of privacy notices being buried in excessively long documents or obfuscated by legalese, but does not solve the problem of data subjects being unable to reasonably foresee the consequences of giving consent.

In order to address this issue to some degree, GDPR provides that an array of information must all be given to data subjects where personal data is collected from them and where they do not already have that information. This information includes, inter alia, contact details of those holding the data, the purposes for which the data is being processed and the legal basis for its processing, how long the data will be stored for, whether it will be used for automated decision-making (including profiling), meaningful information about the logic of any automated decision-making process and the significance and

[60] Article 29 Data Protection Working Party, 2014, p.26
[61] GDPR, art.7(2)
[62] GDPR, art.7(4)

potential consequences of that activity in certain cases, and information on the right to withdraw consent at any time[63] (data processors will be obliged to delete personal data if the data subject withdraws consent[64]). The obligation to provide this information also extends to situations where personal data is inferred through profiling[65]. In those cases, information must be provided within one month of the inference occurring[66] and must also detail the categories of personal data which have been inferred and the purposes for which such inferred data is to be processed[67].

GDPR's requirement that data subjects be informed about the logic, significance, and consequences of automated decision-making, reflecting a similar but more limited duty under the Data Protection Directive, on the face of it appears to allow for individuals to have more knowledge about the analysis being performed with their data and about what kind of information this could reveal and so would seem to address some issues with algorithmic opacity. However, this requirement is limited to decisions that have legal or similarly significant effects on a data subject[68], which would likely not ordinarily include the provision of targeted advertising[69] (but may include situations where, for example, someone with serious financial difficulties is regularly shown ads for gambling, signs up for those services, and ends up in further debt[70]). It may be the case that extending this to cover decisions other than those which have legal or similarly significant effects would go some way towards addressing algorithmic opacity. Indeed, the Article 29 Working Party says that such an approach should be considered 'best practice'[71]. But the benefit of even this is questionable. Wachter et al argue that what is provided for in GDPR does not amount to a 'right to explanation' of how an automated decision relating a data

[63] GDPR, art.13
[64] GDPR, art.17
[65] GDPR, art.14
[66] GDPR, art.14(3)
[67] GDPR, art.14(1)
[68] GDPR, art.22(1)
[69] Mendoza and Bygrave, 2017; Edwards and Veale, 2017; Article 29 Data Protection Working Party, 2017, p.11
[70] Article 29 Data Protection Working Party, 2017, p.11
[71] Article 29 Data Protection Working Party, 2017, p.13

subject has been made[72], as has been claimed[73], but perhaps only a more limited 'right to be informed' of the broad functionality of the decision making system in general[74]. This view is supported by the Article 29 Working Party's guidelines, which also characterise the 'right to an explanation' as a right to be informed[75]. And Edwards and Veale warn that relying on a right to explanation may at best turn out to be a distraction (not least because providing a satisfactory and readily understandable explanation of machine learning processes may not be possible[76]) and at worst may nurture a new kind of "*transparency fallacy*"[77], similar to the problems with notice and consent, as individuals are "*mostly too time-poor, resource-poor, and lacking in the necessary expertise to meaningfully make use of these individual rights*"[78].

There are major issues with the protection of data and privacy in the era of big data, and specifically around the model of notice and consent, but there are also signs of progress. New legal regimes such as GDPR may go some way towards giving the digital citizen more effective tools for protecting their privacy, their data, and themselves. While GDPR is still fundamentally built around notice and consent, and therefore fails to overcome all of those problems, it does provide some potentially valuable reforms to that regime which may go some way at least towards ameliorating those issues. Indeed, we will now move on to look at how the framework involving GDPR and the proposed ePrivacy Regulation may be able to limit the voter surveillance and microtargeting practices discussed in Chapter 5, before assessing the extent to which the existing ePrivacy Directive may, in light of recent decisions of the CJEU, provide a means to challenge the digital panopticon discussed in Chapter 4.

[72] Wachter et al, 2017
[73] Goodman and Flaxman, 2016
[74] Wachter et al, 2017, p.78
[75] Article 29 Data Protection Working Party, 2017, pp.11-14, p.24
[76] Edwards and Veale, 2017, p.29
[77] Edwards and Veale, 2017, p.1
[78] Edwards and Veale, 2017, p.34

6.2 | Data Protection and Voter Microtargeting

In the UK, political organisations[79] are not allowed to advertise freely on television[80], instead being allocated party political broadcasts slots based on their electoral performance[81]. But other political advertising, including the online microtargeting discussed in Chapter 5, is essentially untouched by advertising regulations[82], and the Electoral Commission's role in regulating non-televisual political advertising, including microtargeting and other online advertising, is limited[83]. However, there are questions about the legality of such voter surveillance and microtargeting by political organisations in the UK under DPA. Indeed, the Information Commissioner's Office ('ICO') announced in March 2017 that it is investigating the use of data in both the 2015 general election and the 2016 Brexit referendum[84]. And in May 2017 the ICO further announced that it will investigate the use of these practices by UK political parties in that year's general election[85]. It remains to be seen what conclusions the ICO will reach in relation to DPA, but GDPR will in May 2018 replace data protection legislation in each Member State, including DPA. So while the ICO is investigating voter surveillance and microtargeting under the existing legal regime, it is perhaps more relevant in terms of future activities to determine the extent to which it may be lawful under GDPR.

To try to answer this question, we will first look at pertinent aspects of the EU's proposed ePrivacy Regulation[86], which will regulate online direct marketing. Although the Regulation is still to be finalised, it is to sit alongside and augment

[79] Meaning here a person or organisation registered with the Electoral Commission under section 23 of the Political Parties, Elections and Referendums Act 2000
[80] Communications Act 2003, s.319; s.321
[81] Communications Act 2003, s.333
[82] Tambini et al, 2017, p.8
[83] Electoral Commission, 2016; while there is a reasonable argument that the Electoral Commission should have a greater role in regulating microtargeting, the fact that these practices are fundamentally grounded in the processing of personal data and make use of commercial behavioural targeting tools (and therefore come within the remit of data protection law) mean that the ICO is perhaps better placed.
[84] Doward et al, 2017
[85] Denham, 2017
[86] Draft ePrivacy Regulation

GDPR. We will then set out the pertinent provisions of GDPR as well as some relevant points from the UK's proposed Data Protection Bill ('DPB'), and in the process will discuss the extent to which these practices will be legally permissible under this regime and in what circumstances this will be the case. Although microtargeting can take place in a number of ways, including over the phone, via email, and through the post, we will focus here on how microtargeted political advertising takes place over the internet on social media sites or elsewhere.

6.2.1 | Microtargeting and the ePrivacy Regulation

We must, due to the restrictions placed on direct marketing, consider whether the microtargeting of voters by political organisations, either directly or through social media, can be considered to fall into that category of activity. DPA defined direct marketing as "*the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals*"[87], and the Information Tribunal found that this includes such activity by political parties[88]. The current legislation regulating direct marketing in the UK is the Privacy and Electronic Communications (EC Directive) Regulations 2003[89] (based on the proposed ePrivacy Regulation's predecessor, the ePrivacy Directive[90]), but the Regulations only place substantive restrictions and requirements on direct marketing through telephone calls[91], fax[92], and email[93] (which, for the purposes of the Regulations, includes SMS[94]) and so are inadequate for addressing the kind of microtargeted political advertising which occurs online and which has developed since their adoption. However, the ePrivacy Regulation will replace existing legislation on this, and may extend to targeted advertising. Article 4 defines direct marketing as "*any form of*

[87] DPA 1998, s.11
[88] *Scottish National Party v Information Commissioner* [2006] UKIT EA_2005_0021
[89] Privacy and Electronic Communications (EC Directive) Regulations 2003 ('2003 Regulations')
[90] ePrivacy Directive
[91] 2003 Regulations, reg.19; reg.21
[92] 2003 Regulations, reg.20
[93] 2003 Regulations, reg.22
[94] 2003 Regulations, reg.2(1)

advertising, whether written or oral, sent to one or more identified or identifiable end-users of electronic communications services, including the use of automated calling and communication systems with or without human interaction, electronic mail, SMS, etc."[95]. There are three issues to consider here – first, the meaning of 'advertising'; second, the meaning of 'identified or identifiable end-user'; and, third, whether microtargeted political advertising is 'sent' to an identified or identifiable end-user.

The first two can be quickly dealt with. The ePrivacy Regulation does not define 'advertising', but its recitals state that direct marketing "*should also include messages sent by political parties that contact natural persons via electronic communications services in order to promote their parties*"[96]. While recitals are not binding they are essential to interpretation, so such activity by political organisations is likely to be considered advertising in this context. And in terms of the meaning of 'identified or identifiable end-user', the Regulation itself is again silent on the definition, but it imports GDPR's definitions where relevant[97]. So 'identifiable end-user' here would have the same definition as in GDPR – i.e. a person who can be identified directly or indirectly, including, but not limited to, by "*a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*"[98].

And microtargeted advertising, whether through social media or not, will almost always be sent to an individual or group of individuals who can be identified in some way, whether directly or indirectly, either through their name, through an identification number (such as a data profile ID number), through an online identifier (such as an IP address), through some combination of the factors specific to the identity of those individuals, and so on. This will be particularly so if individuals are microtargeted using tools such as Facebook's Custom Audiences, which allows advertisers to match Facebook accounts to known

[95] Draft ePrivacy Regulation, art.4(3)(f)
[96] Draft ePrivacy Regulation, recital 32
[97] Draft ePrivacy Regulation, art.4(1)(a)
[98] GDPR, art.4

individuals in their databases and target them specifically and directly. So the ePrivacy Regulation's definition of direct marketing would appear to include microtargeted political advertising, particularly where sent through social media sites, as it will in most cases have been sent to an identified or identifiable end-user (although non-targeted political advertising would not be direct marketing and so would fall outside of the Regulation).

In terms of substance, the ePrivacy Regulation contains restrictions on direct marketing. These include the need for users to opt-in to being contacted[99], except in limited circumstances where contact details have been obtained as part of the sale of goods or services and are being used to make a subsequent offer of similar goods or services and where the recipient has been given the clear and distinct opportunity to opt-out[100]. So, whatever the legal basis for voter surveillance under GDPR, the actual act of contacting voters with microtargeted advertising will in most circumstances require the recipient to have opted-in to being contacted. As well as this, direct marketing must identify itself as such, must state who is sending it, and must inform the recipient of their right to withdraw their consent, in an easy manner, to receiving further communications[101].

6.2.2 | Voter Surveillance and GDPR

We will now set out the relevant provisions of GDPR, and will highlight similarities to and differences from the DPA regime. And, while GDPR has direct effect in EU Member States without further enactment, and while the European Union (Withdrawal) Bill proposes to transfer GDPR into domestic law once the UK has left the EU[102], the Government has proposed the new Data Protection Bill to complement, restrict, or otherwise clarify various provisions of GDPR. At the time of writing the Bill is making its way through Parliament, so is subject to

[99] Draft ePrivacy Regulation, art.16(1)
[100] Draft ePrivacy Regulation, art.16(2)
[101] Draft ePrivacy Regulation, art.16(6)
[102] European Union (Withdrawal) Bill, clause 3

change, but there a few points of significance which will be noted where relevant.

Defining Personal Data

Under GDPR, personal data is "*any information relating to an identified or identifiable natural person*"[103] (with the meaning of 'identifiable natural person' as set out previously). Compared to DPA – which defined personal data as that from which a living person can be identified, either from that data alone or from that data and other data held by the controller[104] – GDPR clarifies the scope of 'personal data' to now explicitly include online identifiers, pseudonymous data, and profiles that allow an individual to be singled out or identified[105]. This will include personal data inferred from other personal data, such as through predictive analytics, as long as it relates to an identified or identifiable natural person.

Data Processing Principles

As with DPA, GDPR sets out several principles that apply to the processing of personal data[106]. A few are of particular relevance here. Personal data should only be collected for specified and explicit purposes and not processed in a manner incompatible with those purposes (known as 'purpose limitation')[107]. Such data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')[108]. And personal data should be accurate and kept up to date, and every reasonable step must be taken to ensure that inaccurate data is erased or rectified without delay ('accuracy')[109].

[103] GDPR, art.4(1)
[104] DPA 1998, s.1(1)
[105] GDPR, recital 26; recital 30
[106] GDPR, art.5 GDPR
[107] GDPR, art.5(1)(b)
[108] GDPR, art.5(1)(c)
[109] GDPR, art.5(1)(d)

Rights of the Data Subject

GDPR, like DPA, provides that where personal data is processed for direct marketing the data subject has the right to object to such processing[110], explicitly including automated profiling where related to such marketing[111]. And, reflecting the position in the draft ePrivacy Regulation, GDPR provides that this right should be explicitly brought to the data subject's attention and presented clearly and separately from any other information when the data subject is first contacted[112]. The data subject also has the right to withdraw consent at any time, whatever the purpose of the processing, and should be informed of that right when consent is requested. Withdrawing consent should be as easy as giving it[113]. Controllers will be obliged to delete personal data if the data subject withdraws consent[114].

GDPR further provides that various information must be given to data subjects where personal data is collected from them. This includes, inter alia, contact details of those holding the data, the purposes for which the data is being processed and the legal basis for its processing, how long the data will be stored for, whether it will be used for automated decision-making (including profiling) and meaningful information about the logic, significance, and potential consequences of that decision-making, and about the right to withdraw consent at any time[115]. Substantively the same information should be provided to data subjects when personal data relating to them is obtained from sources other than directly from the data subject, including where it has been inferred[116]. In these cases, the data subject should also be informed of where the data has come from[117] and the categories of personal data concerned[118]. Where personal data hasn't been directly obtained from the data subject, whether through

[110] GDPR, art.21(1)
[111] GDPR, art.21(2)
[112] GDPR, art.21(4)
[113] GDPR, art.7(3)
[114] GDPR, art.17
[115] GDPR, art.13
[116] GDPR, art.14
[117] GDPR, art.14(2)(f)
[118] GDPR, art.14(1)(d)

inference or otherwise, the above information should be provided within one month of the data being obtained by the controller[119]. All of the required information should be provided to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language[120].

Data subjects have a variety of further rights[121]. These include a right of access to personal data, including the right to be told whether personal data concerning them is being processed, and a right to rectification of inaccuracies. They have a right to erasure of personal data (the 'right to be forgotten'), which applies in a number of circumstances including, inter alia, where the personal data is no longer relevant to the purposes for which it was collected and where the data subject withdraws consent to processing. Data subjects also have right to the restriction of processing where the accuracy of data is disputed, and the right to receive personal data concerning them and to transmit that data to another controller (the 'right to portability'). The data subject also has the right to object to processing which is undertaken in the pursuit of the controller's legitimate interests, including profiling, and explicitly where data is processed for the purposes of direct marketing.

When Personal Data Can Be Processed

As in DPA, personal data under GDPR can be one of two varieties – 'ordinary' or 'sensitive' (i.e. data which falls into one of the 'special categories' of personal data[122]). The special categories include data which reveals political opinions or religious or philosophical beliefs, which are obviously relevant to political campaigns, but also other categories of data which may be of use to political organisations including on racial or ethnic origin, trade union membership, sex life, and sexual orientation[123].

[119] GDPR, art.14(3)
[120] GDPR, art.12(1)
[121] GDPR, arts.15-19; 21
[122] GDPR, recital 10
[123] GDPR, art.9(1)

There are several ways that personal data could be considered sensitive. The first and most straightforward – reflecting the position in DPA – is where personal data obviously falls into one of the special categories and was collected directly from a voter, either by a political organisation itself or by a third party (which we can call 'directly sensitive data'). This could be, for example, information on how someone voted at a previous election, on how they intend to vote at the next election, or relating to their opinion on a particular political issue, but could also be information falling into any other special category. The second, going beyond DPA, is where apparently ordinary personal data 'reveals' information which falls into a special category ('potentially sensitive data'). This includes personal data which is not itself sensitive, but from which information falling into one of the special categories can be inferred[124]. The third, which also goes beyond DPA, relates to personal data that has been inferred. Where that inferred data falls into a special category – for example, if profiling infers a voter's political beliefs – then that inferred data will itself be considered sensitive data[125] ('inferred sensitive data'), since personal data is any information relating to an identified or identifiable person and sensitive data is a subset of personal data.

GDPR also sets out several conditions, not found in DPA, around obtaining valid consent[126]. These include that the controller must be able to demonstrate that the data subject consented to processing for the purpose being pursued. GDPR also states that if requests for consent are given in the context of a written declaration then that request must be clearly distinguishable from other parts of the declaration and must be made in an intelligible and easily accessible form, using clear and plain language, otherwise consent will not be binding. In assessing whether consent is freely given, utmost account shall be taken of whether the provision of a service is conditional on consent to the processing of personal data that isn't necessary for the provision of that service.

[124] Bennett 2016, p.266; Article 29 Data Protection Working Party, 2011, p.6
[125] GDPR, recital 60
[126] GDPR, art.7

Further restrictions on the processing of ordinary and sensitive personal data also apply. And, like DPA, GDPR contains greater restrictions on the processing of sensitive personal data than on ordinary personal data. We will discuss ordinary and sensitive personal data in turn.

Ordinary Personal Data

GDPR contains similar restrictions to DPA on the processing of ordinary personal data. As well as the principles of purpose limitation and data minimisation, personal data can be processed only where one of a number of conditions is met. These include where the data subject has consented to the processing, where the processing is necessary for a task carried out in the public interest, or where the processing is necessary for the purposes of the legitimate interests of the data controller or a third party[127]. GDPR says that the question of what can be considered to be in the public interest is to be determined by further EU or domestic law[128]. To this end, DPB says that tasks in the public interest in this context do not include activities by political parties[129]. So there are essentially two grounds under which the processing of ordinary data by political organisations will be lawful.

The first is with the data subject's consent. In this case, processing by political organisations will be lawful if the data was collected for specified political purposes and the processing otherwise complies with the requirements applicable to processing personal data. In practice, this means that so long as data is obtained either by a political organisation or by a third party with the consent of the data subject for political purposes then processing by a political organisation for those purposes will be lawful (so long as, if they obtain the data from a third party, they do so lawfully and meet the relevant requirements as to the provision of information to the data subject). But it should be noted that the processing of personal data for the purposes of political microtargeting may

[127] GDPR, arts.5-7
[128] GDPR, art.6(2)-(3)
[129] DPB, clause 7

constitute a distinct purpose from commercial or other purposes. So social media sites which gather data on their users in the UK, which allow political organisations to make use of their microtargeted advertising systems, and which rely on this ground should make it clear to those users that their data is likely to be processed for political purposes as well as for the commercial purposes for which it is gathered.

The second is if processing is necessary for the purposes of legitimate interests pursued by the data controller. Recital 47 states that direct marketing may be considered to be a legitimate interest[130], which provides a guide to what this may encompass in this context. If this ground applies then ordinary data obtained not for political purposes (whether obtained by a political organisation or by a third party) could be lawfully processed by political organisations for the purposes of microtargeted advertising, and social media sites could process ordinary personal data for use in the microtargeting tools that they provide to political organisations. If this is indeed the case, then the GDPR right to object to the processing of personal data, including profiling, in the context of direct marketing would also apply, as would the requirements that the data subject be furnished with an array of information when data is collected from them or within one month of the data being obtained from elsewhere (including information on what the data is to be used for and on their right to object). However, the Article 29 Data Protection Working Party has said, in the context of the Data Protection Directive, that merely having a legitimate interest in processing personal data does not necessarily mean that the processing is lawful[131]. They emphasise that whether the legitimate interests ground applies will depend on balancing the rights of the data subject against the legitimate interests of the controller, a point which is carried through to GDPR[132]. And they make clear that extensive surveillance of a data subject without their consent in order to build up a detailed profile of them involving data from many different sources is likely to present a significant intrusion into the data subject's privacy,

[130] GDPR, recital 47
[131] Article 29 Data Protection Working Party, 2014, p.25
[132] GDPR, art.6(1)(f)

in which case the legitimate interest would be overridden by the interests and rights of the data subject[133]. So while this ground may apply where political organisations are involved in relatively limited surveillance practices, it is not likely to be open to those involved in more extensive surveillance or to social media sites.

The position set out so far is limited to ordinary personal data. Given that much of the information that may be of interest to political organisations is considered sensitive, the usefulness to political organisations of these grounds for processing may be somewhat limited. And whatever ground is relied on for processing ordinary data the ePrivacy Regulation will also apply to microtargeted advertising based on that data, including its requirements that the communications identify themselves as marketing, identify who has sent the communication, and inform the individual of their right to withdraw their consent to further communications. We now turn to the question of using sensitive personal data, which may be of more use.

Sensitive Personal Data

As with DPA, the processing of sensitive data is prohibited unless an exemption is met[134]. Most of the ten specified exemptions – such as where processing is necessary to protect the vital interests of a data subject who is physically or legally incapable of giving consent, or where processing is necessary for the purposes of preventative or occupational medicine – can be easily discounted so far as political organisations are concerned. There are in fact only four which may be relevant in this context. The first is that the data subject has explicitly consented to the processing for political purposes[135]; the second is that the data subject is a member or former member of the political organisation or is in regular contact with it[136]; the third is that processing is necessary for reasons of

[133] Article 29 Data Protection Working Party, 2014, p.26
[134] GDPR, art.9(1)
[135] GDPR, art.9(2)(a)
[136] GDPR, art.9(2)(d)

substantial public interest[137]; and the fourth is that the data has been manifestly made public by the data subject[138]. We will deal with each of these in turn.

The first exemption is that the data subject has explicitly consented to processing for political purposes. This exemption is available to political organisations, and, unlike the other exemptions, also to social media sites that process sensitive data and provide microtargeting tools to political organisations. Given the need for *explicit* consent, the need for data controllers to be able to demonstrate that consent has been given, and the requirements around requests for consent made in writing, it is difficult to see how the processing of inferred sensitive data could be permissible under this exemption. And if social media sites gather or infer information about the political beliefs of users, or any other sensitive data, including potentially sensitive data, and provide this information to political organisations for the purposes of microtargeted advertising, or otherwise use it in relation to the microtargeted advertising tools that they provide to political organisations, then this use for political purposes should be explicitly brought to the data subject's attention and data subjects should give explicit consent to the data's processing for that purpose. Further, if a political organisation is using these tools to microtarget voters based on ordinary personal data provided to it by the social media site (say, for example, targeting 25 year old married women in London on the basis that it believes that this demographic is likely to be receptive to its message, or targeting specific individuals that it has selected using its own analysis) then this doesn't necessarily remove the need for an exemption to be met – it may simply move the point at which it is required. While the social media site will need to have gained consent to the processing of ordinary data for political purposes, in relation to the processing that led the political organisation to conclude that those voters would be worth targeting the political organisation might itself need to meet either the explicit consent exemption or one of the others that could apply.

[137] GDPR, art.9(2)(g)
[138] GDPR, art.9(2)(e)

The second exemption is that the data subject is a member or former member of the political organisation in question or is in regular contact with it in connection with its political purposes. This can only apply where processing is carried out in the course of the organisation's legitimate activities, and provided the data is not disclosed to a third party without the subject's consent. As discussed previously, 'legitimate interests' include direct marketing, so, assuming that 'interests' and 'activities' are two sides of the same coin, 'legitimate activities' seems to permit political parties to process the sensitive data of members or former members for microtargeting. But for individuals who do not fall into that category it's unclear what it means for a political organisation to have 'regular contact' with them in connection with its political purposes, and there is no case law on the meaning of the same language in either DPA or the Data Protection Directive. But the ICO says, in relation to the same wording in DPA, that 'regular' does not necessarily mean 'frequent', and that the exemption will apply where an organisation is providing activities or support to the same individuals on an ongoing basis, even if some only contact the organisation once[139]. If this standard is applied similarly in GDPR then it seems likely that this exemption will not be available in most cases.

The third exemption is that processing is necessary for reasons of substantial public interest. This only applies where the processing is done on the basis of EU or domestic law, is proportionate, and respects the essence of the right to data protection and provides appropriate safeguards. It's worth noting that recital 56 states that "*Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established*"[140]. As noted previously, while recitals aren't binding they are essential to interpretation, yet despite the same wording having been used in the recitals to the Data Protection Directive[141] it is not clear what 'in the course

[139] Information Commissioner's Office, 2014
[140] GDPR, recital 56
[141] Data Protection Directive, recital 36

of electoral activities' means here[142] (whether it means a formal election campaign or campaigning more generally), or what it means for the 'operation of the democratic system' to 'require' a political party to compile personal data on political opinions. And, again, there appears to be no case law which more precisely defines these expressions.

However, we can note that this exemption is applicable only on the basis of EU or domestic law[143]. To this end, DPB establishes that the substantial public interest exemption only applies in the UK to the extent permitted therein[144]. Accordingly, under DPB this exemption will only be available where the data controller has a 'policy document' in place[145]. Policy documents are to set out the data controller's procedures for securing compliance with the data processing principles and to set out their policies relating to the retention and erasure of the data held, and should include an indication of how long personal data is likely to be retained[146]. And, under DPB, political organisations will be permitted to process sensitive data revealing political opinion where necessary for their political activities (explicitly including campaigning, fund-raising, and political surveys) without obtaining explicit consent from the data subject, provided doing so isn't likely to cause substantial damage or substantial distress to a person and provided the data subject hasn't given written notice requesting the organisation cease processing[147]. This exemption would presumably also cover the processing of potentially and inferred sensitive data.

The fourth exemption applies in cases where the data has manifestly been made public by the data subject. The wording 'made public by the data subject' implies that a positive act on the part of the data subject in making the data public is required in order for the exemption to apply. This would include data on publicly accessible registers, websites, forums, or public social media

[142] Bennett, 2016, p.267
[143] GDPR, art.9(2)(g)
[144] DPB, clause 9
[145] DPB, Sch.1, para.5
[146] DPB, Sch.1, para.30
[147] DPB, Sch.1, para.17

profiles[148]. So the processing of sensitive data scraped from sources such as these would be permissible under this exemption.

The substantial public interest exemption appears to be the strongest available to a political organisation that wishes to process sensitive personal data for its own surveillance and microtargeting operations. But it should always be borne in mind that even where an exemption is relied upon the ePrivacy Regulation will in most cases require that the recipient of political emails or microtargeted advertising has consented to being contacted, and will likely require microtargeted advertising to identify itself as marketing, to identify who has sent the advertising, and to inform the recipient of their right to withdraw consent to future contact (the latter of which is also provided for in GDPR). And, of course, under any exemption political organisations will be required to inform data subjects that they are processing sensitive data relating to them, and will be required to provide information about a variety of things, including, but not limited to, about the purposes for which data is being processed and about the right to object to the processing. Additionally, where the data hasn't been obtained directly from the data subject, such as where it has been inferred, obtained from a third party, or scraped from social media sites, the data subject will need to be informed about the source of the data and the categories of sensitive data involved.

6.2.3 | The Legal Framework in Practice

It appears that neither the draft ePrivacy Regulation nor GDPR *in principle* prevent political organisations from themselves processing personal data in order to microtarget voters, as long as the applicable restrictions and obligations are complied with.

Where processing ordinary data for political purposes, political organisations and social media sites which provide microtargeting tools will in many cases be

[148] Voigt and von dem Bussche, 2017, p.113

able to rely on either the consent ground (provided the requirements around consent have been complied with) or, for more limited surveillance practices, the legitimate interests ground. But ordinary personal data does not include data falling into any of the special categories, many of which will be useful to political organisations. So the processing of ordinary data may not in practice be of much benefit to political organisations. For the processing of sensitive data, including potentially sensitive data, political organisations may find the explicit consent and substantial public interest exemptions to be the most useful. But they may also in more limited circumstances be able to rely on the exemptions for members, former members, and individuals with whom they are in regular contact, as well as the exemption for data manifestly made public. And social media sites which provide microtargeting tools to political organisations are likely to only be able to rely on the explicit consent exemption, so should make clear to users that their data is to be used for political purposes and obtain explicit consent to that activity. If a consent-based ground for processing is relied on then the request for consent will need to have been presented clearly, in an easily intelligible form, and distinct from any other text, and the fact of consent having been granted will need to be demonstrable. And whatever the legal basis for processing, organisations will also need to comply with the data processing principles, including purpose limitation, data minimisation, and accuracy.

Where personal data is being processed by political organisations, whatever the legal basis for the processing, those organisations will need to provide a variety of information to data subjects. If they have obtained the data directly from data subjects then this information will need to be provided at the time, and if the data is obtained from other sources – either from a third party or through inference – then they will need to provide the same information to data subjects within one month, as well as additional information on the categories of data being processed, on the purpose of the processing, and on the data subject's right to object to further processing. And where microtargeted advertising is sent to end-users – which in most case will only be permissible with the consent of the recipient – the communications will need to identify themselves as direct

marketing, will need to identify the sender of the communication, and will need to inform the recipient of their right to withdraw their consent to further contact.

And voters have further rights in relation to these practices. Above all, they have the right to withdraw consent to processing where it was granted, and the right to object to the further processing of data relating to them which is done on the basis of another ground or exemption. They also have the right to be told whether political organisations are processing data concerning them, the right of access to the data being processed, the right to correct inaccuracies, and the right to require that data relating to them is erased where it is no longer relevant to the purposes for which it was collected, where consent to its processing has been withdrawn, or where the data subject has objected to processing (the 'right to be forgotten').

In all, the framework to be established by GDPR and the draft ePrivacy Regulation restricts the ability of political organisations to undertake voter surveillance and microtargeting, whether directly themselves or making use of the tools provide by social media sites. It also places obligations on political organisations and on those social media sites to limit the purposes for which they use data, to provide information to voters who are being surveilled, and, in most cases, to gain consent from voters to being contacted with political emails or microtargeted advertising. And the rights of data subjects in theory provide ways for voters to resist the forms of control represented by voter surveillance and microtargeting, which seek to adopt the algorithmic governmentality of surveillance capitalism for political ends and thus to appropriate the agency of the digital citizen as a political actor for the benefit of political organisations. However, given that GDPR does not come into force until May 2018, and given that neither the ePrivacy Regulation nor DPB have yet been finalised and are therefore subject to change, whether in practice this framework will have the effect of limiting these voter surveillance and microtargeting practices and empowering the digital citizen remains to be seen.

6.3 | Challenging the Digital Panopticon

We saw in Chapter 4 how the State's online surveillance activities have created a digital panopticon, in which everyone who participates in the digital world is rendered visible, watchable, and potentially subject to control. Providing a legal basis for this, the Investigatory Powers Act[149] ('IPA') received Royal Assent in November 2016. IPA was hailed by the Government as bringing the UK's surveillance framework into the 21st Century and better allowing security and intelligence agencies ('SIAs') to combat terrorism and serious crime[150].

IPA does represent something of an improvement in that it replaces patchwork of frameworks – which included, among others, the Telecommunications Act 1984, the Regulation of Investigatory Powers Act 2000, and an array of practices of uncertain or questionable legal basis – with one piece of legislation which puts these practices on an identifiable legal footing with some limitations on their undertaking and which contains a relatively coherent oversight regime in the form of the Judicial Commissioners. But IPA itself raises a range of concerns, with its progress through Parliament marked by sustained opposition from civil liberties groups as well as pointed criticism from Parliament's committees. For example, the Intelligence and Security Committee criticised the draft Bill's lack of emphasis on privacy[151], described the approach towards examination of communications data as "*inconsistent and largely incomprehensible*"[152], and concluded that the draft Bill was "*handicapped from the outset*"[153] in terms of its ability to provide a clear and comprehensive framework governing surveillance powers. The Joint Committee on the draft Bill criticised it extensively[154], opining that it was likely incompatible with ECHR[155] and failed to provide effective safeguards[156] and making over 80

[149] Investigatory Powers Act 2016 ('IPA 2016')
[150] Home Office, 04/11/2015
[151] Intelligence and Security Committee, HC 795, paras 8-9
[152] Intelligence and Security Committee, HC 795, para H
[153] Intelligence and Security Committee, HC 795, para 4
[154] Joint Committee on the Draft IP Bill, HL Paper 93/HC 651
[155] Joint Committee on the Draft IP Bill, HL Paper 93/HC 651, para 331
[156] Joint Committee on the Draft IP Bill, HL Paper 93/HC 651, para 406, paras 438-439, para 450, para 457, paras 510-511, paras 574-575

recommendations for changes (most of which were not taken up when the Bill itself was published less than a month after the Committee's report was published). The House of Commons Science and Technology Committee said the draft Bill caused "*confusion*"[157], highlighted "*widespread doubts over the definition, not to mention the definability*"[158] of key terms, raised concerns over the difficulty of separating metadata from content data[159], and warned that the Bill risked undermining the UK's technology sector[160].

While these provide a background to IPA in terms of the debate which occurred over the adequacy of the Bill as a comprehensive legal framework for state surveillance and highlight with the Bill (many of which were not remedied in the final Act), our focus here is on the ability of the law to provide an effective challenge to one of the most controversial aspects of IPA – the bulk communications data retention and disclosure framework in Parts 3 and 4. This establishes a legal regime in which the internet history of everyone in the UK can potentially be captured, stored, and disclosed to public authorities – including police and SIAs, but also a range of other public bodies – upon request, with such requests requiring the approval of neither the Home Secretary nor a judge. Taking the data retention and disclosure provisions of IPA in the context of two recent decisions of the CJEU relating to the ePrivacy Directive which addressed previous communications data retention frameworks, we will look at how EU law standards provide opportunities for challenging the digital panopticon. We will first distil the requirements set by the CJEU, and will then proceed to examine IPA's framework for compatibility with those requirements in terms of both retention of and access to communications data.

[157] Science and Technology Committee, HC 573, paras 30-31, para 43, para 75
[158] Science and Technology Committee, HC 573, p.3
[159] Science and Technology Committee, HC 573, para 16
[160] Science and Technology Committee, HC 573, p.3

6.3.1 | *Digital Rights Ireland* and *Watson*

Between 2009 and 2014, Internet Service Providers ('ISPs') served notice by the Home Secretary[161] were required to store some communications data for 12 months[162] under the Data Retention (EC Directive) Regulations 2009 ('the 2009 Regulations'), pursuant to the Data Retention Directive[163] ('DRD'). This involved retaining metadata[164] rather than the content of communications. In 2014, the CJEU found in *Digital Rights Ireland*[165] ('*DRI*') that DRD was incompatible with Articles 7 (respect for private and family life, including privacy of communications[166]) and 8 (protection of personal data[167]) of the EU's Charter of Fundamental Rights[168] ('the Charter'). As a result, the Data Retention and Investigatory Powers Act[169] ('DRIPA') was quickly passed in order to pre-empt challenges to the 2009 Regulations based on *DRI*. The High Court subsequently followed *DRI* to find that section 1 DRIPA was incompatible with the Charter and the Government was given until April 2016 before it would be disapplied[170]. The Court of Appeal indicated that it was minded to disagree with the High Court but referred to the CJEU for a preliminary ruling for clarification[171]. In December 2016 the CJEU in *Watson*[172] confirmed the incompatibility of DRIPA-style retention (in any case, DRIPA was subject to a sunset clause meaning that it would be automatically repealed on 31st December 2016[173] – this was the impetus behind IPA). *DRI* and *Watson* together provide the requirements in EU

[161] Data Retention (EC Directive) Regulations 2009 ('2009 Regulations'), reg.10
[162] 2009 Regulations, regs.4-5
[163] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54 ('Data Retention Directive')
[164] 2009 Regulations, reg.2; Sch.1, Pt 3
[165] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* [2015] QB 127
[166] Charter of Fundamental Rights, art.7
[167] Charter of Fundamental Rights, art.8
[168] Charter of Fundamental Rights of the European Union ('Charter of Fundamental Rights')
[169] Data Retention and Investigatory Powers Act 2014 ('DRIPA 2014')
[170] *David Davis and others v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin)
[171] *Secretary of State for the Home Department v David Davis and others* [2015] EWCA Civ 1185
[172] *Tele2 Sverige AB v Post-och telestyrelsen, Secretary of State for the Home Department v Tom Watson and others* [2017] 2 WLR 1289
[173] DRIPA 2014, s.8(3)

law to which IPA must conform both in terms of the retention of communications data and in terms of access to retained data.

DRI considered the validity of DRD in relation to Articles 7 and 8 of the Charter read alongside Article 52(1), which states that for interferences with Charter rights to be potentially justifiable they must respect the essence of those rights[174]. The CJEU held that legislation permitting the retention only of metadata and requiring measures be adopted to protect the security and integrity of retained data does not adversely affect the essence of Articles 7 and 8, respectively, and so constitutes a potentially justifiable interference with those rights[175]. According to *DRI*, retention may be justified provided it satisfies an objective of general interest[176] (such as, but not necessarily limited to, fighting serious crime or terrorism[177]), and is limited to what is strictly necessary to pursue the objective[178]. Access to retained data for the purpose of fighting crime should be limited only to offences determined by objective criteria to be sufficiently serious to justify the interference with Articles 7 and 8[179]. Access should also be subject to prior review by a court or independent administrative body[180].

Watson addressed the question of the compliance of bulk data retention with the ePrivacy Directive, read alongside Articles 7, 8, and 52(1) of the Charter[181]. In doing so the CJEU drew the purposes for which data may be retained narrower than in *DRI* to include only national security, defence, public security[182], and serious crime[183]. The court also went much further than *DRI* in finding that in order to be proportionate retention must be an exception rather than the rule[184], as well as being limited to what is strictly necessary for the

[174] Charter of Fundamental Rights, art.52(1)
[175] *DRI* [2015] QB 127 at [39]-[40]
[176] *DRI* [2015] QB 127 at [38]
[177] *DRI* [2015] QB 127 at [42]
[178] *DRI* [2015] QB 127 at [46], [52]
[179] *DRI* [2015] QB 127 at [60]
[180] *DRI* [2015] QB 127 at [62]
[181] *Watson* [2017] 2 WLR 1289 at [62]
[182] *Watson* [2017] 2 WLR 1289 at [90]
[183] *Watson* [2017] 2 WLR 1289 at [102]
[184] *Watson* [2017] 2 WLR 1289 at [104]

purpose being sought[185]. *Watson* also addressed the question of requirements for access to retained data[186]. The court found that the purposes for which retained data can be accessed must genuinely and strictly correspond to the same purposes for which it can be retained[187]. In order to be proportionate, access to retained data must be limited to what is strictly necessary[188]. In order to ensure that this is the case, access must normally be subject to prior review by a court or an independent administrative body[189]. Further, persons whose data has been accessed should be notified as soon as doing so would not jeopardise an investigation[190].

Seven requirements can broadly be distilled from *DRI* and *Watson* that IPA must satisfy. The first four relate to retention under Part 4. These are that retained data must exclude content, that ISPs must be required to ensure the security and integrity of retained data, that the purpose being sought by retention can only extend to national security, defence, public security, and fighting serious crime, and that retention must be proportionate with data retained as an exception rather than as the rule and only to the extent strictly necessary for the purpose being sought. The final three relate to obtaining data under Part 3. These are that access to data must be only for a purpose genuinely and strictly corresponding to those for which it can be retained, that in order to be proportionate data can be accessed only to the extent strictly necessary, and that there are required safeguards and oversight mechanisms.

6.3.2 | Communications Data Retention under IPA

Part 4 IPA provides for the bulk retention of communications data. ISPs who have been served a retention notice are required to retain all relevant

[185] *Watson* [2017] 2 WLR 1289 at [96]
[186] *Watson* [2017] 2 WLR 1289 at [114]
[187] *Watson* [2017] 2 WLR 1289 at [115]
[188] *Watson* [2017] 2 WLR 1289 at [116]
[189] *Watson* [2017] 2 WLR 1289 at [120]
[190] *Watson* [2017] 2 WLR 1289 at [121]

communications data covered by the retention notice sent from devices connected to their network for a maximum of 12 months[191].

The Nature of Retained Data

DRI established that legislation permitting the acquisition of knowledge of the content of a communication would be contrary to the essence of Article 7 of the Charter and thus unjustifiable[192]. Retention must therefore not include the content of communications in order to be a potentially justifiable interference with Article 7.

The data that ISPs may be required to retain under IPA is 'relevant communications data'[193]. This is defined as a subset of communications data that identifies the sender or recipient of a communication; the time or duration of a communication; the type, method, pattern, or fact of communication; the system from, to, or through which a communication is transmitted; or the location of any such system[194]. Communications data includes certain types of entity data and events data, on one hand, and explicitly excludes the content of communications, on the other[195]. As communications data excludes content, the first step in determining whether retention is in fact contrary to the essence of Article 7 is to look at how IPA defines content.

Under IPA content in this context is any element of a communication, or data attached to or associated with a communication, which reveals anything that might reasonably be considered to be the meaning of that communication[196]. This does not include any meaning arising from the mere fact of the communication having occurred or from data relating to the transmission of the communication. This may be compared with the definition of relevant communications data under DRIPA, which excludes data revealing the content

[191] IPA 2016, s.87
[192] *DRI* [2015] QB 127 at [39]
[193] IPA 2016, s.87(1)
[194] IPA 2016, s.87(11)
[195] IPA 2016, s.261(5)
[196] IPA 2016, s.261(6)

of a communication[197], rather than the meaning. It seems that in replacing DRIPA Parliament has chosen not to carry over a definition that excludes content generally from communications data, instead providing one that excludes only the meaning of a communication. However, it is not clear precisely what the 'meaning' of a communication extends to. It is also not clear that data revealing the meaning of a communication is the same as data providing knowledge of its content. It is quite conceivable that there could be elements of a communication that provide knowledge of its content, and so would be impermissible to retain per *DRI*, but do not reveal its *meaning* and so would not be considered to be content for the purposes of IPA. This could be, for example, a telephone number conveyed in the body of an email (i.e. providing knowledge of some of the content), but not text surrounding it that relates to it and provides context (i.e. revealing the meaning of the email).

It is not clear that all data providing knowledge of the content of a communication is explicitly not communications data. So it is necessary to look at what is explicitly included in order to determine whether or not retention under IPA interferes with the essence of Article 7 of the Charter. Entity data is that which is about an entity (a person or a thing[198]) or an association between an entity and a telecommunication system (a system for transmitting communications electronically[199]) or telecommunications service (a service providing access to or use of a telecommunication system[200]) and which identifies or describes the entity[201]. Events data is that which describes an event on, in, or by means of a telecommunication system and consisting of one or more entities engaging in a specific activity at a specific time[202]. The kinds of entity data or events data that may be considered to be communications data include, inter alia, data held by an ISP about a customer and relating to a service provided to them, data included as part of a communication for the purposes of the system by which it is being communicated, and data which is held by an ISP

[197] DRIPA 2014, s.2(2)
[198] IPA 2016, s.261(7)
[199] IPA 2016, s.261(13)
[200] IPA 2016, s.261(11)
[201] IPA 2016, s.261(3)
[202] IPA 2016, s.261(4)

about the architecture of a telecommunication system and is not about a specific person[203]. In this a telephone number in the body of an email would not be events data or entity data and so, while perhaps not content for the purposes of IPA, it would not be considered to be communications data and could not be retained. Communications data therefore appears to include only metadata – relating to the functioning of telecommunication systems, the provision of telecommunications services, and the transmission of communications – rather than data which would provide knowledge of the content of a communication. As relevant communications data is a subset of communications data, it is also limited to metadata. Retention of metadata is not contrary to the essence of Article 7 and is therefore capable of being justified provided it is for permitted purposes and is proportionate to those purposes.

The Security of Retained Data

DRI held that legislation providing for bulk data retention must set out rules for protecting the data retained by ISPs. These must require a high level of protection and security be applied to the data and require the data to be irreversibly destroyed at the end of the retention period[204]. They should also require retained data to be kept within the EU, and compliance must be subject to review by an independent authority as per Article 8 of the Charter[205]. *Watson* restated these four requirements[206].

IPA requires that ISPs must destroy data once its retention is no longer authorised under Part 4, provided its retention isn't otherwise authorised by law[207]. Destruction may take place at monthly or shorter intervals as appear to the ISP to be reasonably practicable[208]. The Information Commissioner must review ISPs' compliance with requirements under Part 4 relating to the

[203] IPA 2016, s.261(5)
[204] *DRI* [2015] QB 127 at [67]
[205] *DRI* [2015] QB 127 at [68]
[206] *Watson* [2017] 2 WLR 1289 at [122]-[123]
[207] IPA 2016, s.92(2)
[208] IPA 2016, s.92(3)

integrity, security, or destruction of retained data[209]. To that extent IPA meets the requirements of *DRI* and *Watson*. However, in terms of the level of protection applied to retained data and the requirement data be kept in the EU, IPA is not in compliance.

Section 92 IPA covers the integrity and security of data retained by ISPs. Retained data is required to be "of the same integrity, and subject to at least the same security and protection"[210] as data on the system from which it is derived. The storage and processing of that data is regulated by the Privacy and Electronic Communications (EC Directive) Regulations 2003[211]. Regulation 5 thereof requires that ISPs take "appropriate"[212] technical and organisational measures, which must at least ensure that data can be accessed only by authorised personnel (a requirement repeated in IPA[213]) for legally authorised purposes[214]. It also requires that data must be protected against "accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure"[215] (again a requirement repeated in IPA[216]). Regulation 5(4) defines 'appropriate' in this context. A measure is appropriate where, taking into account the state of technological developments and the cost of implementation, it is proportionate to the risks being safeguarded against[217]. However, *DRI* requires that when securing retained data ISPs are to ensure a particularly high level of protection and security without regard to economic considerations[218]. As such, the requirement that ISPs secure retained data with the same security and protection as data on the system from which it is derived does not meet the standard set by the CJEU. Further, IPA does not require that data retained by ISPs be kept within the EU. The Data Protection Act 1998 places restrictions on the transfer of personal

[209] IPA 2016, s.244
[210] IPA 2016, s.92(1)(a)
[211] Privacy and Electronic Communications (EC Directive) Regulations 2003 ('2003 Regulations')
[212] 2003 regulations, reg.5(1)
[213] IPA 2016, s.92(1)(b)
[214] 2003 Regulations reg.5(1A)(a)
[215] 2003 Regulations reg.5(1A)(b)
[216] IPA 2016, s.92(1)(c)
[217] 2003 Regulations reg.5(4)
[218] *DRI* [2015] QB 127 at [67]

data to countries outside the EEA[219], which would include relevant communications data insofar as it permits the individual to whom the data relates to be identified[220]. But *Watson* says that the legislation permitting retention must itself provide for retained data to be kept within the EU[221]. This means that relying on other legislation, such as the Data Protection Act, is not permissible.

As IPA fails to meet these requirements, the storage of retained data by ISPs provided for by IPA constitutes an unjustifiable interference with Article 8 of the Charter.

Purposes for Which Data May be Retained

Watson held that data retention is only permissible for a limited number of purposes as permitted by the ePrivacy Directive read in conjunction with Articles 7 and 8 of the Charter. Article 5(1) of the ePrivacy Directive says that as a general rule a user's data may not be stored by another person without the consent of that user[222]. This is subject to exceptions permitted by Article 15(1) of that directive (explicitly including data retention) for various purpose including to safeguard national security, defence, and public security, and for fighting crime[223]. Acknowledging that the interference with Articles 7 and 8 of the Charter posed by bulk data retention is "very far-reaching and…particularly serious"[224], *Watson* held that in terms of fighting crime only the purpose of fighting *serious* crime is a permissible exception[225].

Section 87(1) IPA provides that retention notices may require an ISP to retain relevant communications data for one of the purposes set out in section

[219] DPA 1998, Sch.1, para.8
[220] DPA 1998, s.1(1)
[221] *Watson* [2017] 2 WLR 1289 at [122]
[222] ePrivacy Directive, art.5(1)
[223] ePrivacy Directive, art.15(1)
[224] *Watson* [2017] 2 WLR 1289 at [100]
[225] *Watson* [2017] 2 WLR 1289 at [102]

61(7)[226]. While these purposes include national security and fighting crime[227], this is not limited only to serious crime. Further, section 61(7) sets out a variety of other purposes including, among others, protecting public health, assessing or collecting any taxes or duties payable to government departments, preventing death or injury, assisting investigations into alleged miscarriages of justice, assisting in identifying someone who is deceased or otherwise unable to identify themselves, and the regulation of financial services markets[228]. Accordingly, the purposes for which data can be required to be retained under IPA go beyond those which are permitted by *Watson*.

Proportionality of Data Retention

The principle of proportionality requires that limitations on Articles 7 and 8 of the Charter are permitted only so far as they are strictly necessary[229]. As such, *DRI* and *Watson* both set out requirements that must be met in order for a retention regime to be strictly necessary and thus proportionate.

DRI requires that retention legislation provides clear and precise rules governing the scope and application of interferences with Charter rights[230], and established two grounds for determining the strict necessity of data retention. The first is that retention cannot cover all persons, all means of electronic communication, and all communications data without any differentiation, limitation or exception and cannot cover people for whom there is no evidence capable of suggesting that they have a link, even indirectly or remotely, with serious crime[231]. Additionally, retention must include safeguards for data subject to professional confidentiality, and must require a relationship between the data being retained and a threat to public security[232]. In particular, the latter

[226] IPA 2016, s.87(1)
[227] IPA 2016, s.61(7)(a)-(b)
[228] IPA 2016, s.61(7)(c)-(j)
[229] *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy* [2010] All ER (EC) 213 at [56]; *Volker und Markus Schecke GbR v Land Hessen* [2012] All ER (EC) 127 at [77]
[230] *DRI* [2015] QB 127 at [54]
[231] *DRI* [2015] QB 127 at [57]-[58]
[232] *DRI* [2015] QB 127 at [58]-[59]

means that retention should be limited to a particular time period, geographical location, or circle of people likely to be involved in serious crime, or to people for whom the retention of their data could contribute to fighting serious crime. The second ground is that the period of time for which data is to be retained should distinguish between types of data based on their possible usefulness[233]. The length of the retention period should be based on objective criteria to ensure that it is limited to what is strictly necessary[234].

Watson found that "general and indiscriminate retention"[235] as the rule rather than the exception[236], covering all users without differentiation, limitation, or exception according to the objective pursued[237], and not requiring any particular relationship between the data to be retained and the purpose of retention[238], "exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society"[239]. The requirement that retention must be an exception rather than the rule goes beyond the limits established in *DRI*, which permitted such bulk retention provided the required limitations and exceptions were clearly set out. *Watson* says that legislation must place retention itself as an exception to the general rule set out in Article 5 of the ePrivacy Directive. As such, and while the judgment says that *targeted* retention is permissible provided it is limited to what is strictly necessary[240], the result of *Watson* is that bulk data retention can never be considered to be strictly necessary and thus can never be proportionate.

IPA fails to meet the proportionality requirements of either *DRI* or *Watson*. Retention notices may be tailored to an extent, including by requiring that only data which meets a certain description[241] or is from a certain time period[242] is

[233] *DRI* [2015] QB 127 at [63]
[234] *DRI* [2015] QB 127 at [64]
[235] Watson [2017] 2 WLR 1289 at [97]
[236] *Watson* [2017] 2 WLR 1289 at [104]
[237] *Watson* [2017] 2 WLR 1289 at [105]
[238] *Watson* [2017] 2 WLR 1289 at [106]
[239] *Watson* [2017] 2 WLR 1289 at [107]
[240] *Watson* [2017] 2 WLR 1289 at [109]-[111]
[241] IPA 2016, s.87(2)(b)
[242] IPA 2016, s.87(2)(c)

retained. But section 87 does allow for ISPs to be required to retain "all data"[243] indiscriminately, without differentiation, limitation, or exception, and without clear safeguards for data subject to professional confidentiality. Further, section 87 does not require any relationship between data to be retained and the purpose being pursued or any link between that data and a threat to public security. Nor does it require the retention period, while limited to a maximum of 12 months[244], to be determined based on objective criteria and limited to what is strictly necessary. Finally, section 87 does not set out clear and precise rules on the scope and application of retention. Instead the Secretary of State can issue notices containing "other requirements, or restrictions, in relation to the retention of data"[245] and making "different provision for different purposes"[246]. As such, section 87 does not provide only for retention that is justified as a strictly necessary and therefore proportionate interference with Articles 7 and 8 of the Charter as per *DRI*. Perhaps most significantly, IPA allows for bulk retention as the rule rather than the exception, exceeding the limits of what can be considered strictly necessary, and so cannot be proportionate as per *Watson*.

6.3.3 | Access to Communications Data

Part 3 IPA provides for the disclosure of communications data to relevant public authorities upon request[247]. Relevant public authorities include those public authorities listed in Schedule 4[248] as well as local authorities[249].

Purposes for Which Data May be Obtained

Watson determined that the purposes for which communications data may be accessed must "genuinely and strictly"[250] correspond to one of those established

[243] IPA 2016, s.87(2)(b)
[244] IPA 2016, s.87(3)
[245] IPA 2016, s.87(2)(d)
[246] IPA 2016, s.87(2)(e)
[247] IPA 2016, Pt.3
[248] IPA 2016, s.70
[249] IPA 2016, s.73
[250] *Watson* [2017] 2 WLR 1289 at [115]

by Article 15(1) of the ePrivacy Directive read alongside Articles 7 and 8 of the Charter, namely national security, defence, public security, and fighting serious crime.

DRI requires that 'serious crime' be defined by objective criteria[251]. In IPA this is defined as offences where an individual with no previous convictions could reasonably be expected to be imprisoned for three years or more, or those that involve violence, result in substantial financial gain, or involve a large number of people acting together for a common purpose[252], satisfying *DRI*'s requirement.

However, communications data can be obtained in the pursuit of several purposes beyond those permitted by *Watson*. These include, among others, for protecting public health, for assessing or collecting any taxes or duties payable to government departments, for preventing death or injury, and for assisting investigations into alleged miscarriages of justice[253]. This does not satisfy the requirement in *Watson* limiting the purposes for which communications data can be obtained.

Proportionality of Disclosure

As with retention, *Watson* holds that access to data must not exceed the limits of what is strictly necessary in order to be proportionate[254]. In particular, this means that legislation must provide clear and precise rules indicating in what circumstances and under which conditions data may be obtained for permitted purposes[255]. Legislation must provide that access normally be granted only to the data of individuals suspected of serious criminality (those suspected of planning, committing, having committed, or being implicated in a serious crime)[256].

[251] *DRI* [2015] QB 127 at [46], [52]
[252] IPA 2016, s.263(1)
[253] IPA 2016, s.61(7)
[254] *Watson* [2017] 2 WLR 1289 at [116]
[255] *Watson* [2017] 2 WLR 1289 at [117]
[256] *Watson* [2017] 2 WLR 1289 at [119]

In terms of the circumstances in which communications data can be accessed under IPA, this can only be for use in a specific investigation or operation[257]. Some communications data takes the form of Internet Connection Records ('ICRs'). These are defined in section 62(7) as the subset of communications data generated or processed by an ISP in the process of supplying an internet connection to a customer that identifies, or assists in identifying, the online service that is being used via that connection (which could be a particular website, email service, messaging service, etc.)[258]. Disclosure of communications data other than ICRs is not limited only to that concerning individuals suspected of any criminality, let alone serious criminality.

Several conditions apply to obtaining ICRs that do not apply to obtaining other communications data. Local authorities may not obtain ICRs in order to access data that can only be obtained through ICRs[259]. For public authorities that are not local authorities, ICRs may only be disclosed where one of three conditions is met[260]. The first is that it is necessary to identify unknown persons or devices using a known internet service, but this is not limited to individuals suspected of serious criminality[261]. The second relates to obtaining data for purposes other than fighting crime[262]. The third, which does relate to the purpose of fighting crime, is that obtaining an ICR is necessary either to determine which service is being used, when it is being used, and how it is being used by a person or device whose identity is known, or to determine where or when a known person or device is accessing or running software which involves making available or acquiring material whose possession is a crime[263]. However, this third condition is not limited only to the purpose of fighting *serious* crime, but also to 'other relevant crime'[264]. As such, ICR disclosure is also not limited only to those of

[257] IPA 2016, s.61(1)
[258] IPA 2016, s.62(7)
[259] IPA 2016, s.62(1)
[260] IPA 2016, s.62(2)
[261] IPA 2016, s.62(3)
[262] IPA 2016, s.62(4)
[263] IPA 2016, s.62(5)
[264] IPA 2016, s.62(6)

individuals who are suspected of serious criminality, and is therefore not limited only to what is strictly necessary.

The communications data disclosure framework established by IPA does not therefore provide for a proportionate interference with fundamental rights.

Safeguards and Oversight

Both *DRI* and *Watson* require that requests for access normally be subject to prior review by a court or an independent administrative body[265]. This is to ensure that access to communications data is limited to what is strictly necessary. *Watson* further required that persons whose data has been accessed be notified once it is possible to do so without jeopardising an investigation[266]. IPA does not provide for individuals whose data has been disclosed to be notified.

Requests from local authorities for disclosure of communications data require the approval of a judge[267], and so meet the required standard. But requests for data from public authorities other than local authorities can normally be authorised by senior officers within the requesting authority without requiring approval by a judge[268] (although the approval of a Judicial Commissioner is required for authorisations that would identify a journalistic source[269]). Senior officers may not normally grant authorisations for investigations they are working on[270], and there are certain procedural requirements[271]. And before a senior officer within a relevant public authority can approve a request they must normally consult a Single Point of Contact ('SPoC'), an individual within the authority responsible for advising others internally on requests[272]. SPoCs

[265] *DRI* [2015] QB 127 at [62]; *Watson* [2017] 2 WLR 1289 at [120]
[266] *Watson* [2017] 2 WLR 1289 at [121]
[267] IPA 2016, s.75
[268] IPA 2016, ss.61-66
[269] IPA 2016, s.77
[270] IPA 2016, s.63
[271] IPA 2016, s.64
[272] IPA 2016, s.76

advise on issues including the lawfulness of proposed authorisations, whether it is reasonably practicable to obtain the data sought, and any cost implications of a request[273].

In order to determine whether in terms of public authorities other than local authorities the approval regime satisfies the requirements of *Watson* it is necessary at this point to attempt to determine what the CJEU may mean by 'independent' in this context. The CJEU has previously discussed this[274] in relation to the requirement for independent oversight of compliance with the Data Protection Directive[275]. In that instance the court concluded that 'independent' normally means "a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure"[276]. In its view supervisory authorities "must act objectively and impartially. For that purpose, they must remain free from any external influence"[277]. The CJEU went on to say that this "precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task"[278]. Independence in the context of supervision of data protection, relevant to both the ePrivacy Directive and to Article 8 of the Charter and thus to access to retained data under IPA, appears to require both objectivity and impartiality, and, to that end, freedom from any external influence. The Communications Data Draft Code of Practice says that SPoCs provide "objective judgement"[279], but the code does not require SPoCs to act impartially. The code also states that senior officers shall take account of the SPoC's advice in assessing the necessity of an authorisation[280]. SPoCs do not, however, have the power to block requests and are themselves permitted to authorise requests if they are also senior officers[281].

[273] IPA 2016, s.76(5)-(6)
[274] *European Commission v Germany* [2010] 3 CMLR 2
[275] Data Protection Directive
[276] *Germany* [2010] 3 CMLR 2 at [18]
[277] *Germany* [2010] 3 CMLR 2 at [25]
[278] *Germany* [2010] 3 CMLR 2 at [30]
[279] Home Office, *Communications Data Draft Code of Practice*, 2016, para.4.33
[280] Home Office, *Communications Data Draft Code of Practice*, 2016, para.4.19
[281] IPA 2016, s.76(8)

As such, it seems that in relation to public authorities other than local authorities the framework is not compatible with the requirements established in *DRI* and *Watson* that access to communications data be subject to independent prior review.

Part 3 IPA therefore does not provide the safeguards required to ensure that access to communications data is limited to what is strictly necessary and therefore proportionate to the purpose being sought.

6.3.4 | Locating the Investigatory Powers Act

Bulk communications data retention was a feature of the State surveillance regimes exposed by Edward Snowden, and IPA is the digital panopticon enshrined in law. Rather than establishing a surveillance regime that balances privacy and security concerns, targets those suspected of serious crimes rather than the whole population, and gives due consideration to oversight and accountability issues, the Act gives legal approval to the new technologies of power of the digital panopticon. The digital panopticon renders us all visible, and, as discussed previously[282], panoptic uncertainty – the knowledge that at any point in time you *could* be being watched and the uncertainty of never knowing for sure whether you are or not which results from the "*asymmetrical gaze*"[283] – is enough to regulate behaviour and is key to the effectiveness of the panopticon[284]. This imbalance of knowledge created by the imbalance of visibility leads to an imbalance of power between the watched and the watcher inherent in all surveillance, and through the surveillance of our online lives in the digital panopticon formalised in law by IPA this imbalance is writ large.

However, as we have seen, there are serious issues with the compatibility of the communications data retention and disclosure framework established under IPA with EU law. While retention does appear to be limited to metadata, Parts 3

[282] 4.1.2
[283] Lyon, 1994, p.65
[284] Lyon, 1994, p.65

and 4 IPA do not meet other requirements established by the CJEU. IPA does not require a particularly high level of protection be applied to retained data or that it be kept within the EU. Retention notices can be issued in pursuit of a range of purposes other than those permitted. Retention is indiscriminate and is the rule rather than the exception. The length of the retention period is not objectively determined and limited to what is strictly necessary. IPA does not provide clear and precise rules governing the scope and application of retention. Retained data can be accessed for a variety of purposes other than those permitted. Access is not limited to data of individuals suspected of serious criminality. Finally, the oversight regime does not provide for independent prior review or for individuals whose data has been accessed to be notified when appropriate. Parts 3 and 4 IPA are therefore an unjustifiable interference with Article 15(1) of the ePrivacy Directive read alongside Articles 7 and 8 of the Charter. EU law privacy and data protection standards thus offer a potential route to challenging IPA on a number of grounds. Indeed, in June 2017 Liberty was given permission to contest the compatibility of the communications data retention provisions of IPA with the requirements of EU law[285].

6.4 | Conclusion

In this chapter have seen that online surveillance poses serious challenges for privacy and data protection law, and that while reform is under way this does not go far enough. However, we have also seen that these laws do provide restrictions, do provide some tools to limit and challenge surveillance, and may be of some use to digital citizens in attempting to resist the overlapping forms of corporate, State, and political control to which they are exposed online. What is clear is that the 'notice and consent' model of privacy protection no longer works. While GDPR does reform this model to some degree, there is an extent to which this is simply papering over the cracks. Notice and consent, despite being a failed model, is still the foundation of GDPR, so further reform is necessary if

[285] Liberty, 2017

data protection law is to be an effective protection for the rights of the digital citizen.

That said, GDPR and existing protections are still of use. GDPR, along with the proposed ePrivacy Directive, may limit some surveillance and microtargeting practices by political organisations. The obligations that they impose on political organisations to provide a wealth of information to data subjects, including clearly setting out their rights and how they can be exercised, and the means that they provide for voters to resist these practices by exercising those rights, including to object to the processing of personal data and to withdraw consent to being targeted with advertising, may go some way towards empowering voters. And the existing ePrivacy Directive, alongside the rights to privacy and data protection established in the EU's Charter of Fundamental Rights and the requirements established by the CJEU, provides a means for challenging some aspects of the digital panopticon. In particular, the communications data retention and disclosure provisions of the Investigatory Powers Act, which are commonly known as the 'snooper's charter', seem to be incompatible with these requirements in a number of ways, and are therefore incompatible with EU law.

Chapter 7 | Conclusions and Further Research

Beginning as an academic research project in the 1960s, the internet has come to transform global society. But it has also brought new forms of control, primarily based around the surveillance of the big data produced as people go about their lives in the digital world. Surveillance is data collection for the purpose of influencing or managing the behaviour of those whose data has been gathered[1], and has long been a part of human society. Emerging in the digital world, dataveillance (as understood in this thesis) is a variety of surveillance that involves the surveillance of people using digital information management systems[2]. Dataveillance involves datafication, the process of turning everyday life into quantified data for use in those systems[3], and this thesis discusses dataveillance regimes of two varieties and their impact on the digital citizen. The first, employed by corporations and made use of by political organisations, involves predictive algorithmic analysis of big datasets describing the datafied lives and behaviours of tens or hundreds of millions of people in order to identify correlations and patterns and so infer information about individuals and predict future behaviour. Once predicted, attempts can be made to influence behaviour in the way desired through the highly personalised and dynamic form of behavioural nudging[4] called 'hypernudge'[5]. This is panspectric dataveillance, or dataveillance involving data describing the behaviour of a spectrum of millions of people that seeks to pre-empt their behaviour[6]. The second form of dataveillance discussed in this thesis is panoptic in nature, in this case involving the gathering of as much information about people's digital lives as possible so as to make them permanently visible to the State's security

[1] Lyon, 2001
[2] Clarke, 1988; Degli Esposti, 2014; see Chapter 1.3
[3] Mayer-Schoenberger and Cukier, 2013
[4] Thaler and Sunstein, 2008
[5] Yeung, 2017a
[6] Palmås, 2011

and intelligence agencies. In this, the digital citizen can potentially be observed at any time, but can never know whether at any given time they are actually being observed or not. In theory, this is enough to regulate their behaviour, as they will need to behave acceptably at all times in case they are being observed at any time[7]. We can recognise both of these forms of dataveillance as examples of algorithmic regulation, which is any form of regulatory governance system involving algorithmic decision making[8]. These forms of dataveillance, facilitated by the datafication of our everyday lives as they become increasingly digital, have become key forms of control in the digital world, used by corporations, the State, and political organisations to influence the behaviour of the digital citizen to their benefit.

Due to the ever-increasing importance of the internet in contemporary society and the extensive use of dataveillance in this way it is important to understand these dataveillance regimes, how they work, and the effect that they have on the relationship between those who use the internet and the corporations, the State, and political organisations who undertake dataveillance. So as to do this, a governmentality framework allows us to move beyond governance theories in order to examine power and control in three components – its rationality (the "*ways of rendering reality thinkable in such a way that it was amenable to calculation and programming*"[9]), its technologies for translating that rationality into reality (the techniques and strategies "*imbued with aspirations for the shaping of conduct in the hope of producing certain desired effects and averting certain undesired events*"[10]), and its subject (the person over whom power is being exercised). Following from Weber[11], Dyrberg[12], Savoie[13], and others[14], we can understand power as the capacity to perform a certain act or to bring about a change in behaviour, or the performance of certain behaviour, in another. This

[7] Foucault, 1991
[8] Yeung, 2017b
[9] Miller and Rose, 2008, p.15
[10] Rose, 1999, p.52
[11] Weber, 1978, p.55
[12] Dyrberg, 1997, p.135
[13] Savoie, 2010, p.4
[14] Morriss, 1987, p.19; p.37, quoting Foucault, 2004b

necessarily involves a desired outcome on the part of those exercising power (a rationality), someone over whom power is being exercised (a subject), and a means by which to bring that desired outcome into reality by using some kind of strategy or technique (a technology of power) to effect a power interaction between those exercising power and those over whom it is being exercised (a process called 'translation'[15]). A governmentality analysis means that we can understand why power is being exercised, how it is being exercised, and what effect it has on those over whom it is being exercised. This allows us to understand the relationship that a power interaction creates between those who are exercising power and those over whom it is being exercised.

In undertaking this analysis this thesis has made several original contributions to knowledge, as follows:

1. The dataveillance-based business model of the dominant corporations in the digital world, identified as surveillance capitalism by Zuboff[16], has been contextualised within surveillance literature and for the first time connected with the algorithmic governmentality described by Rouvroy[17]. In this, datafication through surveillance, hypervisibility through algorithmic analysis, and behavioural modification through hypernudging[18], have for the first time been located within algorithmic governmentality as it is employed in surveillance capitalism[19].

2. The new role for the digital citizen in surveillance capitalism as a produsumer has been identified for the first time, and, building on the analysis provided by Fuchs[20] and on Lazzarato's concept of immaterial labour[21], their work in producing behavioural data has been recognised

[15] Rose and Miller, 1992, p.48
[16] Zuboff, 2015
[17] Rouvroy, 2013; See Chapter 3.1
[18] Yeung, 2017a
[19] see Chapter 3.1.2
[20] Fuchs, 2011
[21] Lazzarato, 1996

as produsumption[22]. Produsumption differs from prosumption in that prosumption involves work through the production and consumption of content where the content itself is what generates surplus value[23], whereas produsumption involves work through the generation of behavioural data, which in surveillance capitalism is what generates surplus value (what Zuboff calls 'behavioural surplus'[24]), as a result of the production and consumption of content (which in surveillance capitalism is usually available for free in order to draw in users who will then produce valuable behavioural data). Produsumption also departs from Marxian analyses of capitalism in that produsumption involves both productive labour and a new form of consumptive labour, by which surplus-generating work is done through consumption of content without the intention to produce what is produced which is required of labour in Marxian analyses[25].

3. The online surveillance programmes undertaken by GCHQ and the NSA have for the first time been identified as a digital panopticon, employing a new technology of power of algorithmic panoptic uncertainty[26]. In this new technology of power, the algorithmic opacity discussed by Burrell[27], Danaher[28], and Pasquale[29] and the predictive power of algorithms when put to use in analysing big datasets means that not only can the digital citizen in the digital panopticon not know when they are being watched (which in a panopticon is what generates panoptic uncertainty, its primary control mechanism), they also can't know how they are being watched or what knowledge about them and their lives has been algorithmically generated through the predictive analysis of the big data describing their lives and those of millions of others. In the digital

[22] See Chapter 3.2.1
[23] See, e.g., Ritzer, 2015; see also Toffler, 1980
[24] Zuboff, 2016
[25] Marx, 1990, p.284; Fuchs, 2017, p.68; Jeon, 2011, p.199
[26] See Chapter 4.1.2
[27] Burrell, 2016
[28] Danaher, 2016
[29] Pasquale, 2015

panopticon, smart machines don't just informate, as Zuboff puts it[30], but act as informers, disclosing otherwise unknown information and elevating the new technology of power of algorithmic panoptic uncertainty above the uncertainty that acts as the control mechanism of a panopticon in the offline world.

4. The incompatibility of the communications data retention and disclosure regime in Parts 3 and 4 of the Investigatory Powers Act[31] (commonly known as the 'snooper's charter'), a key aspect of the digital panopticon, with the ePrivacy Directive[32] in light of the CJEU's decisions in *Digital Rights Ireland*[33] and *Watson*[34] has been established for the first time[35]. This data retention regime potentially requires ISPs in the UK to record a variety of information relating to every communication sent by every device connected to their network, to store this information for up to one year, and to disclose this information to a variety of public authorities, including police and security and intelligence agencies but also many others, upon request, without requiring the approval of either the Home Secretary or a judge. This regime is incompatible with EU law on a number of grounds, including, inter alia, that retention as the rule rather than the exception is indiscriminate and does not distinguish between those suspected of serious crime and others; that the length of the retention period is not limited to what is strictly necessary; that access to retained data can be for purposes other than fighting serious crime; and that there is no prior external review of requests for access to retained data.

[30] Zuboff, 1988
[31] Investigatory Powers Act 2016 Pt.3; Pt.4
[32] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 ('ePrivacy Directive')
[33] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* [2015] QB 127
[34] *Tele2 Sverige AB v Post-och telestyrelsen, Secretary of State for the Home Department v Tom Watson and others* [2017] 2 WLR 1289
[35] See Chapter 6.3

5. The voter surveillance and microtargeting practices undertaken by political organisations have also been located in a governmentality framework for the first time, and contextualised within other dataveillance regimes so as to show how the algorithmic governmentality of surveillance capitalism is repurposed for political ends[36]. The impact of the forthcoming General Data Protection Regulation[37] ('GDPR') and the proposed ePrivacy Regulation[38] on these practices has also been assessed, providing, also for the first time, a legal analysis of the obligations that GDPR and the ePrivacy Regulation will place on political organisations that surveil voters as well as the surveillance capitalism corporations that provide microtargeting tools to them[39].

Beyond these original contributions to knowledge, this thesis has more generally given a governmentality-based account of how the relationship between the digital citizen and corporations, the State, and political organisations is remade in the digital world, with pervasive dataveillance by corporations in surveillance capitalism feeding into extensive dataveillance by the State in the digital panopticon and also into the voter surveillance and microtargeting practices undertaken by political organisations. These are three separate but interrelated and overlapping dataveillance regimes, each operating differently, being undertaken for different reasons, and with different effects on the digital citizen, but resulting in the blurring of the lines between and blending together of corporate, State, and political power, as together they remake the relationship between the digital citizen and society. Ultimately, all three of these dataveillance regimes rely on informational asymmetries and thus the imbalances of knowledge inherent in all surveillance, amplified by

[36] See Chapter 5.2
[37] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 ('GDPR')
[38] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ('Draft ePrivacy Regulation')
[39] See Chapter 6.2

predictive algorithmic analysis of big datasets, creating imbalances of power and therefore facilitating the control of the digital citizen according to the rationalities pursued in each regime. Through this, surveillance capitalism and voter surveillance and microtargeting appropriate the agency of the digital citizen as a social, economic, and political actor and direct it towards corporate and political ends, while the digital panopticon renders the digital citizen a passive subject of surveillance as the State pursues security in the existing order.

Following from Foucault[40], we can understand the state as more than the formal institutions of Government or the State. We can recognise it as a regime of multiple governmentalities of the formal State, business, and civil society, an abstraction of the network of power relations that construct it. In this thesis we have identified, discussed, and contextualised the new dataveillance-based governmentalities that exist to make up the UK's network of power relations in the digital world, and the role of the digital citizen within. As such, we can recognise that the UK is emerging as a surveillance state, characterised by the prevalence of data-producing ICTs as a result of the digital transformation of society and consisting of a regime of multiple dataveillance-based governmentalities. In this emerging surveillance state the digital citizen takes on new roles, in new relationships with corporations, the State, and politics, to their detriment.

As we saw in Chapter 3, surveillance capitalism renders the digital citizen as both a produsumer and a commodity, through the datafication of their lives and their behaviour as a data profile – a 'data double'[41] that stands in for the individual – and the sale of access to that profile on the advertising market. This facilitates their exploitation, as their work done as a produsumer generates surplus value for the corporation, and thus their vast profits, without recompense either for the produsumer's loss of control over their productive

[40] Jessop, 2007, p36 – translating Foucault, 2004b, p.79
[41] Heggarty and Ericson, 2000, p.613

and creative activity[42] or for their loss of control of the surplus stemming from its informational and cultural content. Through algorithmic governmentality surveillance capitalism also involves the appropriation of the sovereignty of the individual as a consumer, in theory the key principle in neo-liberalism[43], so that it can be directed in such a way as to be profitable to the corporation. Through hypernudging, with its high degree of personalisation and continual experimentation, corporations learn how best to influence the digital citizen's behaviour so as to direct it in the way desired. The digital citizen's agency as the sovereign actor in neo-liberalism is thus appropriated, and in selling the commodified produsumer as a data profile on the advertising market the corporation also sells access to the digital citizen's vulnerabilities, determined through experimentation in hypernudging, and the powerful tools for taking advantage of them, in effect selling that agency itself to advertisers. In surveillance capitalism, in short, the digital citizen is broken down to their constituent parts through datafication and predictive analysis[44] and reconstructed as an exploitable, manipulable commodity.

And in Chapter 4 we saw how the digital citizen becomes a passive subject of surveillance in the digital panopticon. Where past mass surveillance regimes needed to actively involve the populace in their own surveillance by recruiting informers, in the digital panopticon the access that security and intelligence agencies have to data through interceptors on internet backbone cables, from data provided to them by surveillance capitalism corporations, through the backdoors that they have placed in hardware, software, and networking equipment, and from other sources, means that they have unprecedented access to a wealth of information about the lives and behaviours of hundreds of millions of people. In the digital panopticon, the relationship of trust between the State and the citizen that underpins the presumption of innocence[45] is replaced with one characterised by undue suspicion, with the digital citizen cast as a potential criminal and potential evidence against them gathered, analysed,

[42] Andrejevic, 2011, p.284
[43] Fellner and Spash, 2014
[44] Deleuze, 1992, p.7
[45] Hadjimatheou, 2013, p.5; see also Nance, 1994; and Campbell, 2010

and stored. The chilling effect of the digital panopticon on freedom of expression, which has repeatedly been empirically demonstrated[46], potentially reduces the willingness of people to seek out information on or put forward ideas that may be thought of as being subversive, extreme, or outside the mainstream, and may particularly affect women and young people, who have historically not often had their voices heard. In the digital panopticon, two of the fundamental norms of democratic society that exist for the benefit of the citizen – the presumption of innocence and freedom of expression – are eroded, and the digital citizen finds themselves cast as a potential criminal who may be unwilling to engage with ideas that challenge the status quo.

Through the voter surveillance and microtargeting practices discussed in Chapter 5 the agency of the digital citizen as a political actor is appropriated and directed in the pursuit of the objectives of political organisations. And the asymmetries in access to extensive voter surveillance between wealthy political organisations and others, as well as the same asymmetry in access to the powerful behavioural modification tools with which to microtarget voters that are available through surveillance capitalism, increases the influence of capital in the electoral process, reinforcing the power gains made by capital through the disciplinary neo-liberal revolution[47], and potentially entrench the political establishment to the detriment of new parties, campaigns, and candidates. These new dataveillance-based forms of political control degrade the online public sphere, which in its idealised Habermasian conception should be a space in which citizens can come together and engage in critical public debate free from coercion[48]. As such, as well as being commodified and exploited in surveillance capitalism, with their social and economic agency directed in pursuit of the goals of corporations, the digital citizen as a political actor becomes subject to powerful new behavioural modification tools as political organisations seek electoral success.

[46] Mathews and Tucker, 2015; Stoycheff, 2016; Penney, 2016; Penney, 2017
[47] Gill, 2000, p.6
[48] Habermas, 1989; Poster, 1995

These changes are facilitated by the neo-liberal nature of digital citizenship as it has emerged in the UK, as we saw in Chapter 2. The governmentality of e-government has encouraged the digital citizen to interact with the digitalised State, facilitating neo-liberal rationalities of the stripped back, smaller state while bringing the locus of government into people's homes and encouraging individuals to interact with the digital world. And the digital citizen engages with consumer forms of online politics as an active citizen, engaged in choice-making between an array of commodified issues and political causes and making use of largely individualist forms of participation[49]. Microtargeted political advertising takes advantage of this by placing commodified issues and political points before voters using carefully crafted messages targeted at voters who the political organisation predicts using algorithmic analysis will be most open to its message, and in doing so attempts to appropriate the agency of the active digital citizen as a political actor to try to ensure that their choice-making is directed in the way desired by the political organisation itself. The digital citizen is also engaged in the individualist self-management required in neo-liberal citizenship[50]. This manifests in two ways. The first is digital management of the physical self through self-tracking apps and devices, which generate a wealth of data on the individual's life and behaviour that can be used in surveillance capitalism. The second is managing the digital self. This involves privacy self-management[51], or the need to actively manage privacy and security online. Individuals adopt a variety of strategies to limit disclosure of information to others, and this forms part of online identity performance[52], whereby the digital citizen actively constructs and performs the version of themselves that they wish to present online. The nature of this identity performance is in part directed by the surveillance capitalism corporations who run the sites on which this takes place, with an emphasis on different aspects of identity on different sites (Facebook prioritises social interaction and personal relationships, for example, while LinkedIn focuses on professional and employment). This is an aspect of the self-commodification expected in the

[49] Dahlberg, 2001
[50] Beck and Beck-Gernsheim, 2001; Bauman 2007, pp.58-59
[51] Solove, 2013
[52] van Zoonen, 2013 – see, e.g., Goffman, 1956; Butler, 1988; Schwartz and Halegoua, 2015

consumer society[53], and forms part of the datafication of the digital citizen and thus their commodification as a data profile on the advertising market, the appropriation of their social and through hypernudging economic agency, and, ultimately, their exploitation.

The neo-liberal nature of digital citizenship means that the digital citizen is held responsible for failing to act out the idealised neo-liberal role of the sovereign actor personally responsible for pursuing their own self-interest[54] – if, for example, they become subject to forms of power that direct their agency away from the pursuit of that self-interest and towards the interests of corporations or political organisations. This places the responsibility for their commodification, their exploitation, the appropriation of their agency, and ultimately their control firmly onto their shoulders. This neo-liberal nature of digital citizenship also means that they are responsible for failing to protect their privacy and their data through the current model of 'notice and consent', despite the role of surveillance, big data, and predictive analytics in undermining that model of protection, as we saw in Chapter 6. Individuals can be re-identified from apparently anonymised datasets[55], and poorly executed predictive analytics raises the possibility of potential privacy harms[56]. Even where analysis is accurate, the potential for algorithmic analysis of big datasets to reveal otherwise unknown information means that it's questionable whether effective notice and consent can truly be given[57]. Beyond this, privacy notices are often excessively long[58] and expressed in obfuscating legalese[59], and requests for consent often may themselves be considered to be deceptive[60]. GDPR will reform this to an extent, and provides some potentially useful tools for the individual to protect their data as well as placing some extra obligations on data controllers and processors, but as it is still fundamentally grounded in a

[53] Bauman, 2007, pp.5-6
[54] Harvey, 2005, p.68
[55] Sweeney, 2000; Narayanan and Shmatikov, 2008; Su et al, 2017
[56] Crawford and Schultz, 2014
[57] Solove, 2013
[58] McDonald and Cranor, 2008
[59] Turow, 2008, p.62
[60] Yeung, 2017a

notice and consent model of protection it can't possibly overcome all of that model's problem. As a result, GDPR, while representing significant progress, is imperfect, and future statutory interventions will likely be needed in order to provide for effective legal protections for individuals beyond notice and consent (although questions of what form that should take are outside of the scope of this thesis). However, once outside of the EU the willingness of the British Government to take legislative measures to limit the practices of surveillance capitalism corporations may be somewhat limited given the reliance of British SIAs on the data gathered and analysed by those corporations. But existing privacy and data protection laws do provide a means to counteract some of the practices discussed in this thesis. As seen previously, GDPR and the proposed ePrivacy Regulation may impose limitations on the voter surveillance and microtargeting practices undertaken by political organisations, while the existing ePrivacy Directive provides grounds on which to challenge the legal basis for key aspects of the digital panopticon.

This analysis undertaken in this thesis, while building on empirical research at points, has been largely theoretical, and has been limited to identifying and examining dataveillance regimes and their effect on the digital citizen rather than on discussing solutions to some of the issues that have been raised along the way. As such, there are opportunities for further research of an empirical nature, as well as for the further research into some of the legal issues and development of some of the theoretical concepts expressed herein. The internet of things, which may grow to play a more prominent role in the surveillance practices discussed herein, provides some of these opportunities. Public perceptions of IoT surveillance as it increasingly moves into public spaces and people's homes is an important area of investigation, as are the challenges of ensuring that IoT devices comply with privacy and data protection law, particularly the forthcoming GDPR and ePrivacy Regulation. Some of the issues with legal compliance for IoT devices relate to their operation in environments where more than one person is interacting with them, or where children are likely to interact with them, and centre on how they can provide a service while avoiding unauthorised disclosure of personal data to someone other than the

data subject and can respect the limitations that apply to the processing of personal data related to children. The effective facilitation of data subject rights and protection of personal data as it moves through interconnected IoT devices and systems also poses a significant challenge which requires much work from a tech-legal viewpoint. While surveillance capitalism is the internet's dominant business model, other approaches may be possible which do not involve pervasive and extensive surveillance of user behaviour and which do not facilitate the associate practices discussed in this thesis but do allow for the provision of similar services. What these alternative approaches may be is a rich area for further research. And as GDPR is still built around a failed 'notice and consent' model of protection, questions of how legal frameworks for privacy and data protection should be constructed in future, while already being discussed by some[61], are an area for significant further research. There are also opportunities for further research into public perceptions of State surveillance, the effect of State surveillance on the presumption of innocence, and on the legal basis for State surveillance practices and their compatibility with GDPR, the proposed ePrivacy Regulation, ECHR, and other instruments. As well as this, State surveillance regimes beyond the UK, such as Ireland's proposed data retention framework, are areas of interest, as are State surveillance systems implemented in more authoritarian states, such as the technologically advanced systems operating in China. There will also be a need for further research into whether GDPR and the ePrivacy Regulation, once they come into force, in practice place limitations on the voter surveillance and microtargeting undertaken by political organisations, and, if so, how effective these limitations are.

As a result of this analysis, this thesis has shown that the extensive dataveillance practices undertaken by corporations, the State, and political organisations, facilitated by the neo-liberal nature of digital citizenship, have remade the relationship between the digital citizen and the state to the detriment of the digital citizen. In this emerging surveillance state, the digital citizen takes on

[61] See, for example, Cate and Mayer-Schoenberger, 2013; Cate et al, 2014; Mantelero and Viciago, 2015; Dean et al, 2016; Mittelstadt, 2017; Taylor et al, 2017

new roles, as a produsumer in surveillance capitalism and as a passive subject of surveillance in the digital panopticon. The digital citizen becomes commodified as a data profile to be bought and sold on the advertising market, they are exploited as a produsumer of valuable behavioural data, and their agency as a social, economic, and political actor is appropriated by corporations and political organisations and directed towards corporate and political ends. Fundamental norms that exist to protect the citizen and underpin democratic society are eroded, the influence of capital in the electoral process is potentially increased, the public sphere is degraded through new forms of coercion, and legal protections for privacy and data protection are undermined. This thesis has proposed new concepts where necessary to account for these changes, and for the first time has provided a comprehensive governmentality-based account of the changing relationship between the digital citizen and the emerging surveillance state.

Bibliography

Cases

David Davis and others v Secretary of State for the Home Department [2015] EWHC 2092 (Admin), [2015] WLR(D) 318

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources (C-293/12) EU:C:2014:238, [2015] QB 127

European Commission v Germany (C-518/07) EU:C:2010:125, [2010] 3 CMLR 2

Google Spain v Agencia Española de Protección de Datos (AEPD) and González (c-131/12) ECLI:EU:C:2014:317, [2014] WLR(D) 202

In re Facebook Internet Tracking Litigation 5:12-md-02314-EJD (N.D. Cal. Jun. 30, 2017)

Liberty (The National Council of Civil Liberties) and others v Government Communications Headquarters and others [2014] UKIPTrib 13_77-H

Liberty (The National Council of Civil Liberties) and others v The Secretary of State for Foreign and Commonwealth Affairs and others [2015] UKIPTrib 13_77-H

Privacy International v Foreign Secretary and others [2016] UKIPTrib 15_110-CH

Romanian Constitutional Court Decision no 1258 from 8 October 2009

S and Marper v United Kingdom [2008] ECHR 1581

Scottish National Party v Information Commissioner [2006] UKIT EA_2005_0021

Tele2 Sverige AB v Post-och telestyrelsen, Secretary of State for the Home Department v Tom Watson and others (C-203/15, C-698/15) EU:C:2016:970, [2017] 2 WLR. 1289

Roman Zakharov v Russia [2008] ECHR 964

Smith v Maryland 442 U.S. 735 (1979)

Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy (C-73/07) EU:C:2008:727, [2010] All ER (EC) 213

Volker und Markus Schecke GbR v Land Hessen (C-92/09) EU:C:2010:662, [2012] All ER (EC) 127

Woolmington v Director of Public Prosecutions [1935] UKHL 1

Legislation

Charter of Fundamental Rights of the European Union [2012] OJ C326/391

Communications Act 2003

Communications Decency Act of 1996, 47 U.S.C. § 230

Data Protection Act 1998

Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data 95/46/EC [1995] OJ L281/31)

Data Retention and Investigatory Powers Act 2014

Data Retention (EC Directive) Regulations 2009 (SI 2009/859)

Data Retention and Investigatory Powers Act 2014

Data Retention Directive (Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54)

Draft ePrivacy Regulation (Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC)

ePrivacy Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37)

European Convention on Human Rights 1950

European Union (Withdrawal) Bill (HC Bill 5, 2017-19)

General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1)

Intelligence Services Act 1994

Investigatory Powers Act 2016

Political Parties, Elections and Referendums Act 2000

Police Act 1997

Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426)

Regulation of Investigatory Powers Act 2000

Telecommunications Act 1984

UN General Assembly, Universal Declaration of Human Rights, 1948, Paris

Official Publications, Reports, etc.

Anderson, D., *Report of the Bulk Powers Review*, Cm 9326, August 2016

Article 29 Data Protection Working Party, *Advice paper on special categories of data ("sensitive data")*, April 2011

Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 844/14/EN WP 217, 09/04/2014

Article 29 Data Protection Working Party, *Guidelines on the right to data portability*, 16/EN WP 242, 13/06/2016

Article 29 Data Protection Working Party, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), 17/EN WP 247, 04/04/2017

Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17/EN WP 251, 03/10/2017

European Parliament, "DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", *Committee on Civil Liberties, Justice and Home Affairs*, 09/06/2017

Home Office, *Factsheet – Bulk Equipment Interference*, 31/10/2015 [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473753/Factsheet-Bulk_Equipment_Interference.pdf]

Home Office, *Operational Case for the Retention of Internet Connection Records*, 04/11/2015

Home Office, *Communications Data Draft Code of Practice*, Autumn 2016

House of Commons Hansard, 15/07/2014, Vol. 584, Col. 704

House of Lords Hansard, 11/11/2014, Vol. 757, No. 56, Col. WA24

House of Commons, Science and Technology Committee, *Investigatory Powers Bill: Technology Issues*, The Stationary Office, 2015, HC Paper 573, Session 2015/16 [http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf]

House of Commons Science and Technology Committee, "Investigatory Powers Bill: Technology issues - oral evidence", *HC Paper 573-i*, 10/11/2015

House of Lords Select Committee on the Constitution, "Surveillance: Citizens and the State", *Volume I: Report*, The Stationary Office, 2009, Session 2008/09, HL Paper 18-I

House of Lords Select Committee on the Constitution, "Surveillance: Citizens and the State", *Volume II: Evidence*, The Stationary Office, 2009, Session 2008/09, HL Paper 18-II

Intelligence and Security Committee of Parliament, "Report on the draft Investigatory Powers Bill", *HC Paper 795*, 09/02/2016

Joint Committee on the Draft Investigatory Powers Bill, *Report*, The Stationary Office, 2016, HL Paper 93/ HC Paper 651, Session 2015-16 [http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf]

United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*, A/HRC/23/40, 17/04/2013

Other

Acquisti, A., Brandimarte, L, and Lowenstein, G., "Privacy and human behaviour in the age of information", *Science*, Vol. 347, Issue 6221, 30 January 2015, pp.509-514

Andrejevic, M., "Surveillance and Alienation in the Online Economy", *Surveillance & Society*, Vol. 8, No. 3, 2011, pp.270-287

Andrejevic, M., "Exploitation in the Data Mine", in Fuchs, C., Boersma, K., Albrechtslund, and Sandoval, M. (Eds.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, 2012, New York: Routledge, pp.71-88

Andrejevic, A. and Gates, K. (Eds.), "Big Data Surveillance [special issue]", *Surveillance & Society*, Vol. 12, No. 2, 2014

Angwin, J., "Spy Agency Drowns in Useless Data, Impeding Work, Former Employee Claims", *The Wall Street Journal*, 25/12/2013 [http://www.wsj.com/articles/SB10001424052702304202204579252022823658850]

Anstead, N., "Data-driven campaigning in the 2015 UK general election", *The International Journal of Press/Politics*, 2017 (forthcoming)

Anwer, J, "Users worried about privacy free to leave Facebook, WhatsApp: Facebook lawyer", *India Today*, 28/04/2017 [http://indiatoday.intoday.in/technology/story/users-worried-about-privacy-free-to-leave-facebook-whatsapp-facebook-lawyer/1/940551.html]

Arvidsson, A., "Brands: a critical perspective", *Journal of Consumer Culture*, Vol. 5, No. 2, 2005, pp.235-258

Ayres, A., *Super Crunchers: How Anything Can be Predicted*, 2008, John Murray Publishers

Aviram, A., "Revealed: Bristol's police and mass mobile phone surveillance", *The Bristol Cable*, 10/10/2016 [https://thebristolcable.org/2016/10/imsi]

Bajaj, K., "Cyberspace: Post-Snowden", *Strategic Analysis*, Vol. 38, No. 4, 2014, pp.582-583

Baker, P. M. A., Bricout, J. C., Moon, N. W., Coughlan, B., and Pater, J., "Communities of participation: A comparison of disability and aging identified groups on Facebook and LinkedIn", *Telematics and Informatics*, Vol 30, 2013, pp.22-34

Balkin, J. M., "Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society", New York University Law Review, Vol. 79, No. 1, April 2004

Ball, J., Borger, J., and Greenwald, G, "Revealed: how US and UK spy agencies defeat internet privacy and security", *The Guardian*, 06/09/2013 [https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security]

Ballard, A. O., Hillygus, D. S., and Konitzer, T., "Campaigning Online: Web Display Ads in the 2012 Presidential Campaign", *Political Science & Politics*, Vol. 49, No. 3, July 2016, pp.414-419

Barber, B., "Which Technology in Which Democracy?" in Jenkins, H. and Thorburn, D. (Eds.), *Democracy and the New Media*, 2003, Cambridge, MA: MIT Press

Barry, A., Osbourne, T., and Rose, N., *Foucault and Political Reason: Liberalism, Neoliberalism and rationalities of government*, 1996, Chicago: University of Chicago Press

Bartsch, M. and Dienlin, T., "Control your Facebook: An analysis of online privacy literacy", *Computers in Human Behaviour*, Vol. 56, 2016, pp.147-154

Bauman, Z., *Consuming Life*, 2007, Polity Press

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., and Walker, R.B.J., "After Snowden: Rethinking the Impact of Surveillance", *International Political Sociology*, Vol 8, 2014

BBC News, *Mass snooping fake mobile towers 'uncovered in UK'*, 10/06/2015 [http://www.bbc.co.uk/news/business-33076527]

Beck, U. and Beck-Gernsheim, E., *Individualization: Institutionalized Individualism and Its Social and Political Consequences*, 2001, Sage Publications

Bennett, C., "The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies", *First Monday*, Vol. 18, No. 8. 2013

Bennett, C. J., "Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America?", *International Data Privacy Law*, Vol. 6, No. 6, 2016

Bennett, C. J., Clement, A., and Milberry, K. (Eds.), "Cyber-Surveillance in Everyday Life [special issue]", *Surveillance & Society*, Vol. 9, No. 4, 2012

Beer, D., "The social power of algorithms", *Information, Communication & Society*, Vol. 20, No. 1, 2017, pp.1-13

Bent, O., Dey, P., Weldemariam, K., and Mohinia, M. K, "Modeling user behaviour data in systems of engagement", *Future Generation Computer Systems*, Vol. 68, 2017, pp.456-464

Bentham, J., *The Works of Jeremy Bentham, vol. 4 (Panopticon, Constitution, Colonies, Codification)*, 1843

Besley, T., "Digitized Youth: constructing identities in the creative knowledge economy", Policy Futures in Education, Vol. 8, No. 1, 2010, pp.126-141

Bevir, M. and Rhodes, R., *Interpreting British Governance*. 2003, London: Routledge

Biddle, S., “The NSA leak is real, Snowden documents confirm”, *The Intercept*, 19/08/2016 [https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm]

Big Brother Watch, “Big Brother Watch and Others v UK at the European Court of Human Rights”, *Big Brother Watch Blog*, 03/11/2017 [https://bigbrotherwatch.org.uk/2017/11/big-brother-watch-and-others-v-uk-at-the-european-court-of-human-rights]

Bimber, B., “Digital Media in the Obama Campaigns of 2008 and 2012: Adaptation to the Personalized Communication Environment”, *Journal of Information Technology & Politics*, Vol. 11, No. 2, 2014, pp.130-150

Birchall, C., "Shareveillance: Subjectivity between open and closed data", *Big Data & Society*, 2016

Boas, T., and Gans-Morse, J., “Neoliberalism: from New Liberal philosophy to Anti-Liberal Slogan”, *Studies in Comparative International Development*, Vol 44, No 2, 2009

Bockman, J., “The origins of neoliberalism between Soviet socialism and Western capitalism: “A galaxy without borders””, *Theory and Society*, Vol 36, No 4, Aug 2007, pp.343-371

Bockman, J., “Neoliberalism”, *Contexts*, Vol. 12, No. 3, 2013

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D. I., Marlow, C., Settle, J. E., and Fowler, J H., “A 61-million-person experiment in social influence and political mobilization”, *Nature*, Vol. 489, September 2012, pp.295-298

Borwick, T., “Winning against the odds”, *Kanto Systems: Case Studies* [https://www.kan.to/case-studies]

Brady, H. E., “Political Participation”, in Robinson, J. P., Shaver, P. R., and Wrightsman, L. S. (Eds.), *Measures of Political Attitudes*, 1999, San Diego, CA: Academic Press, pp.737-801

Brennetot, “The geographical and ethical origins of neoliberalism: The Walter Lipmann Colloquium and the foundations of a new geopolitical order”, *Political Geography*, Vol 49, 2015

Bright, P., “2016 sees Internet Explorer usage collapse, Chrome surge”, *ArsTechnica*, 08/01/2017 [https://arstechnica.co.uk/information-

technology/2017/01/2016-on-the-web-firefox-fights-back-as-microsofts-share-slumps]

Brodkin, J., "Websites can keep ignoring "Do Not Track" requests after FCC ruling", *ArsTechnica*, 11/06/2015 [https://arstechnica.com/information-technology/2015/11/fcc-wont-force-websites-to-honor-do-not-track-requests]

Brodkin, J., "Google and Facebook lobbyists try to stop new online privacy protections", *ArsTechnica*, 24/05/2017 [https://arstechnica.com/tech-policy/2017/05/google-and-facebook-lobbyists-try-to-stop-new-online-privacy-protections]

Brown, A., "Facebook is not your friend", *The Guardian*, 14/05/2010 [https://www.theguardian.com/commentisfree/andrewbrown/2010/may/14/facebook-not-your-friend]

Bryant, B., "VICE News Investigation Finds Signs of Secret Phone Surveillance Across London", *VICE News*, 14/01/2016 [https://news.vice.com/article/vice-news-investigation-finds-signs-of-secret-phone-hacking-equipment-across-london]

Bucher, T., "Want to be on top? Algorithmic power and the threat of invisibility on Facebook", *New Media & Society*, Vol. 14, No. 7, 2012, pp.1164-1180

Bucher, T., "The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms", *Information, Communication and Society*, Vol. 20, No. 1, 2017, pp.30-44

Burchell, G., "Pecular interests: civil society and governing 'The system of natural liberty'", in Burchell, G., Gordon, C., and Miller, P. (Eds.), *The Foucault Effect: Studies in governmentality*, 1992, Chicago: University of Chicago Press

Burrell, J., "How the machine 'thinks': Understanding opacity in machine learning algorithms", *Big Data & Society*, January-June 2016, pp.1-12

Burris, S., Kempa, M., and Shearing, C., "Changes in Governance: A Cross-Disciplinary Review of Currrent Scholarship", *Akron Law Review*, Vol. 41, No. 1, 2008

Butler, J., "Performative Acts and Gender Constitution", *Theatre Journal*, Vol. 40, No. 4, 1988, pp.519-531

Callon, M. and Latour, B., "Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologist Help Them To Do So", in Knorr-Cetina, K. and Cicouvel, A.V. (Eds.), *Advances in Social Theory and Methodology*: *Towards an Integration of Micro and Macro-Sociology*, 1981, Boston, pp. 277-303

Cambridge Analytica, *The CA Advantage* [https://ca-political.com/ca-advantage]

Campbell, L, "A rights---based analysis of DNA retention: 'non---conviction' databases and the liberal state", Criminal Law Review, Vol.12, 2010, pp.889-906

Carty, A., "Marxism and International Law: Perspectives for the American (twenty-first) Century?" in Susan Marks (ed), *International Law on the Left: Reexamining Marxist Legacies*, 2008, p.170

Cassidy, R., "How does AdBlock work?", *AdBlock*, 07/09/2016 [https://help.getadblock.com/support/solutions/articles/6000087914-how-does-adblock-work]

Cate, F. H., and Mayer-Schönberger, V., "Notice and consent in a world of Big Data", *International Data Privacy Law*, Vol. 3, No. 2, 2013, pp.67-73

Chadwick, A. and Stromer-Galley, J., "Digital Media, Power, and Democracy in Parties and Election Campaigns: Party Decline or Party Renewal?", *The International Journal of Press/Politics*, Vol. 21, No. 3, 2016, pp.283-293

Charitsis, V., "Prosuming (the) self", *Ephemera*, Vol. 16, No. 3, 2016, pp.37-59

Chin, A. and Klinefelter, A., "Differential Privacy as a Response to the Re-identification Threat: The Facebook Advertiser Case Study", *North Carolina Law Review*, Vol. 90, No. 5, 2012, pp.1418-1455

Chomsky, N., *Profit Over People: Neoliberalism and Global Order*, 1999, New York

Cheng, E., "Amazon climbs into list of top five largest US stocks by market cap", *CNBC*, 23/09/2016 [https://www.cnbc.com/2016/09/23/amazon-climbs-into-list-of-top-five-largest-us-stocks-by-market-cap.html]

Clarke, J., "Consumerism and the remaking of state-citizen relationships", *Paper prepared for ESPAnet conference, Oxford, 9-11 September, 2004* [http://www.spsw.ox.ac.uk/fileadmin/static/Espanet/espanetconference/papers/ppr%5B1%5D.15A.JC.pdf.pdf]

Clarke, R., "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, 1988, pp.498-512

Collier, S. J., "Topologies of Power - Foucault's Analysis of Political Government beyond 'Governmentality'", *Theory, Culture & Society*, Vol. 26, No. 6, 2009, pp. 78–108

Confessore, N. and Hakim, D., "Data Firm Says 'Secret Sauce' Aided Trump; Many Scoff", *The New York Times*, 06/03/2017 [https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html]

Conger, K., "Facebook says it's not making friend suggestions based on your location after all", *TechCrunch*, 28/06/2016 [https://techcrunch.com/2016/06/28/facebook-says-its-not-making-friend-suggestions-based-on-your-location-after-all]

Conger, K., "What Apple's differential privacy means for your data and the future of machine learning", *TechCrunch*, 14/06/2017 [https://techcrunch.com/2016/06/14/differential-privacy]

Connolly, D., "A Little History of the World Wide Web", World Wide Web Consortium, 2000, [https://www.w3.org/History.html]

Constine, J., "Facebook now has 2 billion monthly users…and responsibility", *TechCrunch*, 27/06/2017 [https://techcrunch.com/2017/06/27/facebook-2-billion-users]

Corbett, S. and Walker, A., "The Big Society: Back to the Future", *The Political Quaterly*, Vol. 83, No. 3, July-September 2012

Cormode, G. and Balachander, K., "Key differences between Web 1.0 and Web 2.0", *First Monday*, Vol. 13, No. 6, 2008

Crawford, K., and Schultz, J. M., "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms", *Boston College Law Review*, Vol. 55, No. 93, 2014, p.93-128

Cummings, D., "On the referendum #20: the campaign, physics and data science – Vote Leave's 'Voter Intention Collection System' (VICS) now available for all", *Dominic Cummings's Blog*, 29/10/2016 [https://dominiccummings.com/2016/10/29/on-the-referendum-20-the-

campaign-physics-and-data-science-vote-leaves-voter-intention-collection-system-vics-now-available-for-all]

Cummings, D., "Dominic Cummings: how the Brexit referendum was won", *The Spectator*, 09/01/2017 [https://blogs.spectator.co.uk/2017/01/dominic-cummings-brexit-referendum-won]

Dahlberg, L., "Computer-Mediated Communication and the Public Sphere: A Critical Analysis", *Journal of Computer-mediated Communication*, Vol. 7, No. 1, 2001a

Dahlberg, L., "The Internet and Democratic Discourse: Exploring The Prospects of Online Deliberative Forums Extending the Public Sphere", *Information, Communication & Society*, Vol 4, No. 4, 2001, pp.615-633

Dahlgren, P., "Reconfiguring civic culture in the new media milieu" in Corner, J. and Pels, D. (Eds), *Media and political style: Essays on representation and civic culture*, 2003, pp.151-170, London: Sage

Dahlgren, P., "The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation", *Political Communication*, Vol. 22, No. 2, 2005, pp.147-162

Danaher, J., "The Threat of Algocracy: Reality, Resistance and Accommodation", *Philosophy and Technology*, Vol. 29, 2016, pp.245-268

Davies, H.., "Ted Cruz using firm that harvested data on millions of unwitting Facebook users", *The Guardian*, 11/12/2015 [https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data]

Davis, K., "Tensions of identity in a networked era: Young people's perspectives on the risks and rewards of online self-expression", *New Media & Society*, Vol. 14, No. 4, 2011, pp.634-651

Dean, M., *Governmentality: Power and Rule in Modern Society*, 1999, Sage Publications

Degli Esposti, S., "When big data meets dataveillance: the hidden side of analytics", *Surveillance & Society*, Vol. 12, No. 2, 2014, pp.209-225

DeLanda, M., *War in the Age of Intelligent Machines*, 1991, New York: Zone Books

Deleuze, G., "Postscript on the Societies of Control", *October*, Vol. 59, Winter 1992, pp.3-7

Deloitte, "State of the smart: Consumer and business usage patterns", *Global Market Consumer Survey 2017: UK Cut*, 2017 [https://www.deloitte.co.uk/mobileuk/assets/img/download/global-mobile-consumer-survey-2017_uk-cut.pdf]

Democracy Now, *Vindication for Snowden? Obama Panel Backs Major Curbs on NSA Surveillance, Phone Record Data Mining*, 19/12/2013 [http://www.democracynow.org/2013/12/19/vindication_for_snowden_obama_panel_backs]

Denham, E., "The Information Commissioner opens a formal investigation into the use of data analytics for political purposes", *The Information Commissioner's Office Blog*, 17/05/2017, [https://iconewsblog.org.uk/2017/05/17/information-commissioner-elizabeth-denham-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes]

Dennison, L., Morrison, L., Conway, G., and Yardley, L., "Opportunities and challenges for smartphone applications in supporting health behaviour change", *Journal of International Medical Research*, Vol. 15, No. 4, 2013

Denman, J. and McDonald, P., "Unemployment statistics from 1881 to the present day", *Labour Market Trends*, Office of National Statistics, January 1996 [http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/lms/labour-market-trends--discontinued-/january-1996/unemployment-since-1881.pdf]

Diakopoulos, N., "Algorithmic Accountability Reporting: On the Investigation of Black Boxes", *Tow Center for Digital Journalism: A Tow/Knight Brief*, Columbia Journalism School. 2013 [https://towcenter.org/research/algorithmic-accountability-on-the-investigation-of-black-boxes-2]

DiResta, R., "There are bots. Look around.", RibbonFarm, 23/05/2017 [https://www.ribbonfarm.com/2017/05/23/there-are-bots-look-around]

Doward, J., Cadwalladr, C., and Gibbs, A., "Watchdog to launch inquiry into misuse of data in politics", *The Guardian*, 04/03/2017 [https://www.theguardian.com/technology/2017/mar/04/cambridge-analytics-data-brexit-trump]

Duff, R. A., "Who Must Presume Whom to be Innocent of What?", *Netherlands Journal of Legal Philosophy*, Vol. 42, No. 3, 2013, pp. 170-192.

Duhigg, C., "How Companies Learn Your Secrets", *New York Times*, 16/02/2012 [http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html]

Dwork, C., McSherry, F., Nissim, K., and Smith, A., "Calibrating Noise to Sensitivity in Private Data Analysis", *TCC 2006: Theory of Cryptography*, 2006, pp.265-284

Dyer-Wytheford, N., *Cyber-Marx: Cycles and Circuits of Struggle in High Technology Capitalism*, 1999, University of Illinois Press

Dyer-Wytheford, N., *Cyber-Proletariat: Global Labour in the Digital Vortex*, 2015, Pluto Press

Dyrberg, T. B., *The Circular Structure of Power: Politics, Identity, Community*, 1997, New York

Electoral Commission, *What we do and don't regulate*, 2016 [https://www.electoralcommission.org.uk/our-work/roles-and-responsibilities/our-role-as-regulator-of-political-party-finances/making-an-allegation/what-we-regulate]

Edwards, L. and Veale, M., "Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for", *Duke Law Review*, 2017 (forthcoming) [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855]

Erlingson, U., Pihur, V., and Korolova, A., "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response", *Proceedings of the 21st ACM Conference on Computer and Communications Security*, ACM, 2014 [https://research.google.com/pubs/pub42852.html]

Facebook, *Data Policy*, 29/09/2016 [https://www.facebook.com/about/privacy]

Facebook Business, *Success Story: The Conservative Party* [https://www.facebook.com/business/success/conservative-party]

Facebook Business, *Success Story: Toomey for Senate* [https://www.facebook.com/business/success/toomey-for-senate]

Fakhoury, R. and Aubert, B., "Citizenship, trust, and behavioural intentions to use public e-services: The case of Lebanon", *International Journal of Information Management*, Vol. 35, 2015, pp. 346-351

Farivar, C., "County sheriff has used stingray over 300 times with no warrant", *Ars Technica*, 24/05/2015 [http://arstechnica.com/tech-policy/2015/05/county-sheriff-has-used-stingray-over-300-times-with-no-warrant]

Farrell, G., *The 'Mere Irish' and the Colonisation of Ulster, 1570-1641*, 2017, Palgrave Macmillan

Fellner, W. and Spash, C. L., *The Illusion of Consumer Sovereignty in Economic and Neoliberal Thought*, 2014

Felten, E., "We Are the Product that Facebook Has Been Testing", *Financial Times*, 02/07/2014 [https://www.ft.com/content/6576b0c2-0138-11e4-a938-00144feab7de]

Flood, J., *The Fires: How a Computer Formula, Big Ideas, and the Best of Intentions Burned Down New York City-And Determined the Future of Cities*, 2011, Riverhead Books

Forrest, C., "Android nears 88% global market share, but Apple still makes more money", *TechRepublic*, 04/11/2016 [http://www.techrepublic.com/article/android-nears-88-global-market-share-but-apple-still-makes-more-money]

Fortune, *Biggest Employers* [http://fortune.com/fortune500/list/filtered?sortBy=employees&first500]

Foucault, M., *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977*, 1980, New York: Pantheon Books

Foucault, M., "Technologies of the self", in Martin, L. Gutman, H., and Hutton, P. (Eds.), *Technologies of the Self: A Seminar with Michel Foucault*, 1988, London: Tavistock, pp.16-49

Foucault, M., *The History of Sexuality: An Introduction*, 1990, Penguin

Foucault, M., *Discipline and Punish: The Birth of the Prison*, Trans. A. Sheridan, 1991: Penguin

Foucault, M., "About the Beginning of the Hermeneutics of the Self: Two Lectures at Dartmouth", *Political Theory*, Vol. 21, No. 2, May 1993, pp. 198-227

Foucault, M., *Securite´, territoire, population. Cours au College de France*, 1977 e 1978, 2004a, Paris

Foucault, M.,*Naissance de la biopolitique. Cours au College de France*, 1978 e 1979, 2004b, Paris

Friedman, M., *Capitalism and Freedom*, 1962, Chicago: University of Chicago Press

Friedman, M., and Friedman, R., *Two Lucky People: Memoirs*, 2nd ed., 1998, Chicago: University of Chicago Press

Fuchs, C., "A Contribution to the Critique of the Political Economy of Google", *Fast Capitalism*, Vol. 8, No. 1, 2011

Fuchs, C., "Political Economy and Surveillance Theory", *Critical Sociology*, Vol. 39, No. 5, 2012, pp.671-687

Fuchs, C., "Social Media and the Public Sphere", tripleC, Vol. 12, No. 1, 2014, pp.57-101

Fuchs, C., "The Information Economy and the Labor Theory of Value", *International Journal of Political Economy*, Vol. 46, No. 1, 2017, pp.65-89

Fuchs, C., Boersma, K., Albrechtslund, and Sandoval, M. (Eds.), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, 2012, New York: Routledge

Galetta, A., "The changing nature of the presumption of innocence in today's surveillance societies: rewrite human rights or regulate the use of surveillance technologies?", *European Journal of Law and Technology*, Vol. 4, No. 2, 2013

Galič, M., Timan, T., and Koops, B., "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation", *Philosophy & Technology*, Vol. 30, No. 9, 2017, pp.9-37

Gallagher, R., "From Radio to Porn, British Spies Track Web Users' Online Identities", *The Intercept*, 25/09/2015

[https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities]

Gallagher, R., "Airport Police Demanded an Activist's Passwords. He Refused. Now He Faces Prison in the U.K.", *The Intercept*, 23/09/2017 [https://theintercept.com/2017/09/23/police-schedule-7-uk-rabbani-gchq-passwords]

Gao, G., "What Americans think about NSA surveillance, national security and privacy", *Pew Research*, 29/05/2015 [http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy]

Geiger, R. S., "Does Habermas Understand the Internet? The Algorithmic Construction of the Blogo/Public Sphere", *gnovis: a journal of communication, culture, and technology*, Issue 10, Vol. 1, 2009

Gerlitz, C., and Helmond, A., "The like economy: Social buttons and the data-intensive web", *New Media & Society*, Vol. 15, No. 8, 2013, pp.1348-1365

Gill, S., *The Global Panopticon*, 1995

Gill, S., "The Constitution of Global Capitalism", *International Studies Association Annual Convention, Los Angeles*, Vol. 15, 2000, pp.1-20

Gill, S., *Power and Resistance in the New World Order*, 2nd ed., 2008, New York: Palgrave Macmillan

Gillespie, T., "The Relevance of Algorithms" in Gillespie, T., Boczkowski, P. J., and Foot, K. A. (Eds.), *Media Technologies: Essays on Communication, Materiality, and Society*, 2014, Cambridge, MA: MIT Press, pp.167-193

Giritli Nygren, K., "e-Governmentality: On Electronic Administration in Local Government", *Electronic Journal of e-Government*, Vol. 7, Issue 1, 2009, pp. 55-64

Goldman, E., "The Ten Most Important Section 230 Rulings", *Tulane Journal of Technology & Intellectual Property*, Vol. 20, 2017

Goldman, L., "Statistics and the Science of Society in Early Victorian Britain; An Intellectual Context for the General Register Office", *Social History of Medicine*, Vol. 4, No. 3, 1991, pp.415-434

Goodin, D., "Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts", *ArsTechnica*, 23/06/2014 [https://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts]

Goodin, D., "NSA-leaking Shadow Brokers just dumped its most damaging release yet", *ArsTechnica*, 14/04/2017 [https://arstechnica.com/security/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet]

Glaesar, E. L., and Shleifer, A., "The Rise of the Regulatory State", *Journal of Economic Literature*, Vol. 41, No. 2, 2003, pp.401-425

Goffman, E., *The Presentation of Self in Everyday Life*, 1956, Edinburgh: University of Edinburgh

Goodman, B. and Flaxman, S., "European Union regulations on algorithmic decision-making and a "right to explanation"", *AI Magazine*, Vol. 38, No. 3, 2016

Goodyear, V. A., Kerner, C., and Quennerstedt,M., "Young people's use of wearable health lifestyle technologies; surveillance, self-surveillance and resistance", *Sport, Education and Society*, 2017

Google, "Facts about Google and Competition", *WebArchive* [https://web.archive.org/web/20111104131332/https://www.google.com/competition/howgooglesearchworks.html]

Google, *SOPA/PIPA*, 18/01/2012 [https://www.google.com/doodles/sopa-pipa]

Google, *Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106*, 03/10/2016 [https://ecfsapi.fcc.gov/file/100319291940/2016-10-03%20Google%20Letter%20(WC%2016-106).pdf]

Gordon, C., "Governmental Rationality: An Introduction", in Burchell, G., Gordon, C. and Miller, P. (Eds.), *The Foucault Effect: Studies in Governmentality*, 1991, Chicago: University of Chicago Press

Goss, J., "'We Know Who You Are and We Know Where You Live': The Instrumental Rationality of Geodemographic Systems", *Economic Geography*, Vol. 71, No. 2, April 1995, pp.171-198

Graham, T., Jackson, D., and Wright, S., "'We need to get together and make ourselves heard': everyday online spaces as incubators of political action", *Information, Communication & Society*, 2015

Green, J. and Issenberg, S., "Inside the Trump Bunker, With Days to Go", *Businessweek*, 27/10/2016 [https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go]

Greenwald, G. and MacAskill, E., "NSA Prism program taps in to user data of Apple, Google and others", *The Guardian*, 07/06/2013 [http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data]

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S., and Rushe, D., "Microsoft handed the NSA access to encrypted messages", *The Guardian*, 12/07/2013 [http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data]

Groll, E., "'Shadow Brokers' Claim to be Selling NSA Malware, in What Could Be Historic Hack", *Foreign Policy*, 15/08/2016 [https://foreignpolicy.com/2016/08/15/shadow-brokers-claim-to-be-selling-nsa-malware-in-what-could-be-historic-hack]

Gwynne, A., "Theresa May called a snap election, but we in Labour had Snapchat. No contest", *The Guardian*, 15/06/2017 [https://www.theguardian.com/commentisfree/2017/jun/15/theresa-may-snap-election-labour-snapchat-campaigning]

Habermas, J., *The Structural Transformation of the Public Sphere*, Trans. Burger, T., 1989, Cambridge, MA; MIT Press

Habermas, J., "Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension? The Impact of Normative Theory on Empirical Research", *Communication Theory*, Vol. 16, No. 4, 2006, pp.411-426

Hadjimatheou, K., "Surveillance, the moral presumption of innocence, the right to be free from criminal stigmatisation and trust", *Surveillance: Ethical Issues, Legal Limitations, and Efficiency*, SURVEILLE, European University Institute, 2013

Hadjimatheou, K, "Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence", *Philosophy & Technology*, Vol.30, Issue 1, March 2017, pp.39-54

Halpern, S., "How He Used Facebook to Win", *The New York Review of Books*, 08/06/2017 [http://www.nybooks.com/articles/2017/06/08/how-trump-used-facebook-to-win]

Halvais, A., *Search Engine Society*, 2009, Cambridge: Polity Press

Hansard Society, *Audit of Political Engagement 10: The 2013 Report*, 2013

Hansard Society, *Audit of Political Engagement 14: The 2017 Report*, 2017

Harvey, D., *A Brief History of Neoliberalism*, 2005, Oxford: Oxford University Press

Hay, C., *Why We Hate Politics*, 2007, Cambridge: Polity Press

Hayek, F., "The Dangers to Personal Liberty", *The Times*, July 11 1978 [https://coreyrobin.files.wordpress.com/2012/07/hayek-letter-to-the-times-july-11-1978.pdf]

Hayek, F., *The Road to Serfdom*, 2nd ed., 2001, Routledge

Healey, N., *Britain's Economic Miracle: Myth or Reality?*, 2002, Routledge

Heggarty, K. D. and Ericson, R. V., "The surveillant assemblage", *The British Journal of Sociology*, Vol. 51, No. 4., 2000, pp.605-622

Hendrix, J. and Carroll, D., "Confronting a Nightmare for Democracy: Personal Data, Personalized Media and Weaponized Propaganda", *Medium*, 04/05/2017 [https://medium.com/@profcarroll/confronting-a-nightmare-for-democracy-5333181ca675]

Hern, A., "'Anonymous' browsing data can be easily exposed, researchers reveal", *The Guardian*, 01/08/2017 [https://www.theguardian.com/technology/2017/aug/01/data-browsing-habits-brokers]

Heyer, P., and Crowley, D., "Introduction", in Innis, H. A., *The Bias of Communication*, 1989, Toronto: University of Toronto Press

Hern, A., "Apply blocking ads that follow users around web is 'sabotage'", *The Guardian*, 08/09/2017 [https://www.theguardian.com/technology/2017/sep/18/apple-stopping-ads-

follow-you-around-internet-sabotage-advertising-industry-ios-11-and-macos-high-sierra-safari-internet]

Hewitt, M., "New Labour, Human Nature, and Welfare Reform", in Sykes, R., Bochel, C., and Ellison, N. (Eds.), *Social Policy Review: Developments and Debates: 2000-2001 No.13*¸ 2001, Policy Press

Heyer, P., and Crowley, D., "Introduction", in Innis, H. A., *The Bias of Communication*, 1989, Toronto: University of Toronto Press

Hill, K., "How Facebook Outs Sex Workers", *Gizmodo*, 11/10/2017 [https://gizmodo.com/how-facebook-outs-sex-workers-1818861596]

Hill, R., K., "What an Algorithm Is", *Philosophy and Technology*, Vol. 29, No. 35, 2016, pp.35-59

Hintz, A., and Brown, I., "Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden", *International Journal of Communication*, Vol. 11, 2017, pp.782-801

Hintz, A., Dencik, L, and Wahl-Jorgensen, K., "Digital Citizenship and Surveillance Society", *International Journal of Communications*, Vol. 11, 2017, pp.731-739

HM Revenue & Customs, *HMRC sees biggest digital Self Assessment ever*, 02/02/2015 [https://www.gov.uk/government/news/hmrc-sees-biggest-digital-self-assessment-ever]

Hofacker, C. F., Malthouse, E. C., and Sultan, F., "Big data and consumer behaviour: imminent opportunities", *Journal of Consumer Marketing*, Vol. 33, Issue 2, 2016, pp.89-97

Hood, C., "A Public Management for all Seasons?", *Public Administration*, Vol. 69, Issue 1, March 1991, pp. 3-19

Howard, P. N. and Kreiss, D., "Political parties and voter privacy: Australia, Canada, the United Kingdom, and United States in comparative perspective", *First Monday*, Vol. 15, No. 12, 2010

Hughes, S. S., "US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program", *Canadian Journal of Law and Society*, Vol. 27, No. 3, 2012, pp.399-425

Hull, G., "Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data", *Ethics and Information Technology*, Vol. 17, No. 2, 2015, pp.89-101

Information Commissioner's Office, *The exemption from registration for 'not-for-profit' organisations*, 11/09/2014 [https://ico.org.uk/media/for-organisations/documents/1567/exemption-from-registration-for-not-for-profit-organisations.pdf]

Innis, H. A., *The Bias of Communication*, 1989, Toronto: University of Toronto Press

Isin, E., and Ruppert, E., *Being Digital Citizens*, 2015, Maryland: Rowman & Littlefield

Jarvis, J., "How much data the NSA really gets", *The Guardian*, 13/08/2013 [http://www.theguardian.com/commentisfree/2013/aug/13/nsa-internet-traffic-surveillance]

Jeon, H., "The Value and Price of Information Commodities: an Assessment of the South Korean Controversy", in Zarembka, P. and Desai, R. (Eds.), *Revitalizing Marxist Theory for Today's Capitalism*, 2011, Emerald Books, pp.191-222

Jessop, B., "Hollowing out the 'nation-state' and multilevel governance" in Kennett, P. (Ed.), *A Handbook Of Comparative Social Policy*, 2004, Cheltenham: Edward Elgar Publishing, 2004, pp. 11-25

Jessop, B., "From micro-powers to governmentality: Foucault's work on statehood, state formation, statecraft and state power", *Political Geography*, Vol. 26, 2007, pp. 34-40

Johnson, G. "Can Obama Data-Mine His Way to Victory?", *Chicago Magazine*, 24/07/2012 [http://www.chicagomag.com/Chicago-Magazine/August-2012/Can-Obama-Data-Mine-His-Way-to-Victory]

Johnson-Williams, E., "ISC comes down hard on Investigatory Powers Bill", *Open Rights Group*, 09/02/2016, [https://www.openrightsgroup.org/blog/2016/isc-comes-down-hard-on-investigatory-powers-bill]

Jones, J. J., Bond, R. M., Bakshy, E., Eckles, D., and Foweler, J. H., "Social influence and political mobilization: further evidence from a randomized experiment in the 2012 U.S. presidential election", *PLoS One*, Vol. 12, No. 4, 2017

Jones, M., *An Introduction to Politcal Geography Space, Place, and Politics*, 2007, New York: Routledge

Juniper Research, *AD BLOCKING TO COST PUBLISHERS $27BN IN LOST REVENUES BY 2020*, 11/05/2016 [https://www.juniperresearch.com/press/press-releases/ad-blocking-to-cost-publishers-$27bn-in-lost-reven]

Just, N., and Latzer, M., "Governance by algorithms: reality construction by algorithmic selection on the Internet", *Media, Culture & Society*, Vol. 39, No. 2, 2017, pp.238-258

Kadidal, S., "NSA Surveillance: The Implications for Civil Liberties", *I/S: A Journal of Law & Policy for the Information Society*, Vol. 10, Issue 1, Spring 2014, pp.433-479

Kahneman, D., *Thinking, Fast and Slow*, 2012, Penguin

Kaplan, J., "Improving Enforcement and Transparency of Ads on Facebook", *Facebook Newsroom*, 02/10/2017 [https://newsroom.fb.com/news/2017/10/improving-enforcement-and-transparency]

Katz, J., "Birth of a Digital Nation", *Wired*, 01/04/1997 [https://www.wired.com/1997/04/netizen-3]

Kearney, R., *Modern Movements in European Philosophy: Phenomenology, Critical Theory, Structuralism*, 1994, Manchester: Manchester University Press

Keay, D., "Aids, education and the year 2000!", *Woman's Own*, 31/10/1987, pp.1-45

Kennett, P. A., "Global Perspectives on Governance", in Osborne, S. (Ed.), *The New Public Governance. Emerging Perspectives on the Theory and Practice of Public Governance*, (pp. 19-35), 2010, Routledge

Kimmons, R., "Social Networking Sites, Literacy, and the Authentic Identity Problem", *TechTrends*, Vol. 58, No. 2, 2014, pp.93-98

Kitchin, R., *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, 2014, London: Sage Publications

Kitchin, R., "Thinking critically about and researching algorithms", *Information, Communication & Society*, Vol. 20, No. 1, 2017, pp.14-29

Kitchin, R. and Lauriault, T. P., "Towards critical data studies: Charting and unpacking data assemblages and their work", The Programmable City Working Paper 2, 2014

Klauser, F. R. and Albrechtslund, A., "From self-tracking to smart urban infrastructures: Towards an interdisciplinary research agenda on Big Data", *Surveillance & Society*, Vol. 12, No. 2, 2014, pp.273-286

Klein, *The Shock Doctrine: The Rise of Disaster Capitalism*, 2007, Penguin

Kreiss, D., "Yes We Can (Profile You): A Brief Primer on Campaigns and Political Data", *Stanford Law Review Online*, Vol. 64, 2012

Kosinki, M., Stillwell, D., and Graepel, T., "Private traits and attributes are predictable from digital records of human behavior", *PNAS*, Vol. 110, No. 15, April 2013, pp.5802-5804

Kotz, D., *The Rise and Fall of Neoliberal Capitalism*, 2015, Cambridge, MA: Harvard University Press

Kramer, N. C. and Haferkamp, N., "Online self-presentation: Balancing privacy concerns and impression construction on social networking sites" in Trepte, S. and Reinecke, L. (Eds.), *Privacy Online: Perspectives on privacy and self-disclosure in the social web*, 2011, Berlin: Springer-Verlag, pp.127-142

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T., "Online social networks: why we disclose", *Journal of Information Technology*, 2010, Vol. 25, pp.109-125

Landau, S., "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations", *IEEE Security and Privacy Magazine*, Vol. 11, No. 4, July 2013, pp.54-63

Langley, P. and Leyshon, A., "Platform capitalism: The intermediation and capitalisation of digital economic circulation", *Finance & Society*, Vol. 3, No. 1, 2017

Lankton, N. K., McKnight, D. H., and Tripp, J. F., "Facebook privacy management strategies: A cluster analysis of user privacy behaviors", *Computers in Human Behaviour*, Vol. 73, 2017, pp.149-163

Lapowski, I, “Here’s How Facebook Actually Won Trump the Presidency”, *Wired*, 15/11/2016 [https://www.wired.com/2016/11/facebook-won-trump-election-not-just-fake-news]

Layard, R. and Nickell, S., “The Thatcher Miracle?”, *The American Economic Review*, Vol. 79, No. 2, May 1989, pp. 215-219

Lazzarato, M.. "Immaterial labor”, *Radical thought in Italy: A potential politics*, 1996, pp.133-47.

Lazzarato, M., “Neoliberalism in Action: Inequality, Insecurity and the Reconstitution of the Social”, *Theory, Culture and Society*, Vol. 26, No. 6, 2009, pp.109-133

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., and Wolff, S., “Brief History of the Internet”, *Internet Society*, 1997 [https://www.internetsociety.org/internet/history-internet/brief-history-internet]

Lemke, T., “‘The birth of bio-politics’: Michel Foucault’s lecture at the Collège de France on neo-liberal governmentality”, *Economy and Society*, Vol. 30, No. 2, May 2001, pp. 190-207

Lepri, B., Staiano, J., Sangokoya, D., Letouzé, E., and Oliver, N., "The Tyranny of Data? The Bright and Dark Sides of Data-Driven Decision-Making for Social Good” in Cerquitelli, T., Quercia, D., and Pasquale, F. (Eds), *Transparent Data Mining for Big and Small Data*, 2007, Springer, pp.3-24

Levin, S., “Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless'”, *The Guardian*, 01/05/2017 [https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens]

Liberty, *Liberty’s briefing on Part 6 of the Investigatory Powers Bill for Committee Stage in the House of Commons*, April 2016

Liberty, *Liberty gets go-ahead to challenge Snoopers’ Charter in the High Court*, 30/06/2017 [https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/liberty-gets-go-ahead-challenge-snoopers%E2%80%99-charter-high-court]

Light, J. S., *From Warfare to Welfare: Defense Intellectuals and Urban Problems in Cold War America*, 2005, John Hopkins University Press

Lightfoot, G., and Wisnieski, T. P., "Information asymmetry and power in a surveillance society", *Information and Organization*", Vol. 24, 2014, pp.214-235

Linden, G., Smith, B., and York, J., "Amazon.com Recommendations: Item-to-Item Collaborative Filtering", *IEEE Internet Computing*, January/February 2003, pp.76-80

Lupton, D., "Quantifying the body: monitoring and measuring health in the age of mHealth technologies", *Critical Public Health*, Vol. 23, No. 4, 2013, pp.393-403

Lupton, D., "Self-tracking Modes: Reflexive Self-Monitoring and Data Practices", *Paper for the 'Imminent Citzenships: Personhood and Identity Politics in the Informatic Age' workshop*, ANU, Canberra, 27/08/2014 [http://ssrn.com/abstract=2483549]

Lupton, D., "Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps", *Culture, Health & Sexuality*, Vol. 17, No. 4, 2015, pp.440-453

Lupton, D., "The diverse domains of quantified selves: self-tracking modes and dataveillance", *Economy and Society*, Vol. 45, No. 1, 2016, pp.101-122

Lyon, D., *Electronic Eye: The Rise of Surveillance Society*, 1994: University of Minnesota Press

Lyon, D., *Surveillance Society: Monitoring Everyday Life*, 2001, Milton Keynes: Open University Press

Lyon, D., *Surveillance Studies: An Overview*, 2007, Polity Press

MacAskill, E., "Edward Snowden, NSA files source: 'If they want to get you, in time they will'" [video], *The Guardian*, 10/06/2013 [http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why]

MacAskill, E., Borger, J., and Greenwald, G., "The National Security Agency: surveillance giant with eyes on America", *The Guardian*, 06/06/2013 [http://www.theguardian.com/world/2013/jun/06/national-security-agency-surveillance]

Madden, M., Lenhard, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., and Beaton, M., "Teens, Social Media, and Privacy", *Pew Research Center*, 21/05/2013

Mahon, B., *Knowledge is Power: A Short History of Official Data Collection in the UK*, 2009, Office of National Statistics

Majone, G., "From the Positive to the Regulatory State: Causes and Consequences of Changes in the Mode of Governance", *Journal of Public Policy*, Vol. 17, 1997, pp. 139-167

Mandese, J., "Ad Groups Petition Consumer Internet Privacy Rules, Call Opt-In Requirement 'Onerous'", *MediaDailyNews*, 03/01/2017 [https://www.mediapost.com/publications/article/292165/ad-groups-petition-consumer-internet-privacy-rules.html]

Mantelero, A., "Social Control, Transparency, and Participation in the Big Data World", *Journal of Internet Law*, April 2014, pp.23-29

Manzerolle, V., and Smeltzer, S., "Consumer Databases and the Commercial Mediation of Identity: a medium theory analysis", *Surveillance & Society*, Vol. 8, No. 3, 2011, pp.323-337

Mathews, A., and Tucker, C., "Government Surveillance and Internet Search Behaviour", 29/04/2015 [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2412564]

Marx, K., *A Contribution to the Critique of Political Economy*, 1859

Marx, K., *Capital: A Critique of Political Economy, Vol. 1*, 1990, Penguin Classics

Mayer-Schoenberger, V., and Cukier, K., *Big Data: A Revolution That Will Transform How We Live, Work, and* Think, 2013, London: John Murray Publishers

McDonald, A. M., and Cranor, L. F., "The Cost of Reading Privacy Policies", ISJLP, Vol. 4, 2008, pp.543-58

Mendelson, A. and Papacharissi, Z., "Look at us: collective narcissism in college student Facebook photo galleries" in Papacharissi, Z (Ed.), *A Networked Self: Identity, Community and Culture on Social Network Sites*, 2010, New York: Routledge, pp.251-273

Mendoza, I. and Bygrave, L. A., "The Right Not to Be Subject to Automated Decisions Based on Profiling", in Synodinou, T., Jougleux, P., Markou, C., and Prastitou, T. (Eds.), *EU Internet Law: Regulation and Enforcement*, 2017, Springer International Publishing

Milaj, J., and Bonnici, J. P. M., "Unwitting subjects of surveillance and the presumption of innocence", *Computer Law & Security Review*, Vol. 30, 2014, pp.419-428

Miller, P. and Rose, N., "Governing economic life", *Economy and Society*, Vol. 19, No. 1, 1990, pp.1-31

Miller, P. and Rose, N., *Governing the Present: Administering Economic, Social and Personal Life*, 2008, Polity Press

Moll, R., Pieschl, S., and Bromme, R., "Competent or clueless? Users' knowledge and misconceptions about their online privacy management", *Computers in Human Behaviour*, Vol. 41, 2014, pp.212-219

Montano, J. P., "'Dycheyn and Hegeying': The Material Culture of the Tudor Plantations in Ireland", in Bateman, F. and Pilkington, L. (Eds.), *Studies in Settler Colonialism: Politics, Identity and Culture*, 2011, Palgrave Macmillan

Morison, J., "Gov 2.0: Towards a User Generated State?", *Modern Law Review*, Vol. 73, No.4, 2010, pp.551-577

Morozov, E., *To Save Everything, Click Here: Technology, Solutionism, and the Urge to Fix Problems that Don't Exist*, 2013, Allen Lane

Morriss, P., *Power: A Philosophical Analysis*, 1987, Manchester: Manchester University Press

Mossberger, K., Tolbert, C., and McNeal, R., *Digital Citizenship: The Internet, Society, and Participation*, 2008, Cambridge, MA: MIT Press

Murgia, M., "UK-US pact will force big tech companies to hand over data", *Financial Times*, 21/10/2017 [https://www.ft.com/content/09153a74-b5bc-11e7-aa26-bb002965bce8]

Nance, D., A., "Civility and the Burden of Proof", Harvard Journal of Law and Public Policy, Vol.17, 1994

Narayanan, A., and Shmatikov, V., "Robust De-anonymization of Large Sparse Datasets", *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, 2008, pp.111-125

Noelle-Neumann, E., "The Spiral of Silence: A Theory of Public Opinion", *Journal of Communication*, Vol. 24, Issue 2, June 1974, pp.43-51

Nosko, A., Wood, E., Molema, S., "All about me: Disclosure in online social networking profiles: the case of FACEBOOK", *Computers in Human Behaviour*, Vol. 23, Issue 3, 2010, pp.406-418

Ofcom, *Adults' media use and attitudes: Report 2017*, 2017 [https://www.ofcom.org.uk/__data/assets/pdf_file/0020/102755/adults-media-use-attitudes-2017.pdf]

Office for National Statistics, *Statistical Bulletin: Internet access – households and individuals: 2017*, 03/08/2017 [https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2017]

Olma, S. "Never mind the sharing economy: here's platform capitalism", *Institute of Network Cultures Blog*, 16/10/2014 [http://networkcultures.org/mycreativity/2014/10/16/never-mind-the-sharing-economy-heres-platform-capitalism]

Osborne, D. and Gaebler, T., *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector*, 1992, Perseus Books

O'Mahony, L. F., O'Mahony, D., Hickey, R., *Moral Rhetoric and the Criminalisation of Squatting: Vulnerable Demons?*, 2015, Routledge

O'Reilly, L, "Google, Microsoft, and Amazon are paying AdBlock Plus huge fees to get their ads unblocked", *Business Insider*, 03/02/2015 [http://uk.businessinsider.com/google-microsoft-amazon-taboola-pay-adblock-plus-to-stop-blocking-their-ads-2015-2]

O'Reilly, L., "The Race Is On to Challenge Google-Facebook 'Duopoly' in Digital Advertising", *Wall Street Journal*, 19/06/2017 [https://www.wsj.com/articles/the-race-is-on-to-challenge-google-facebook-duopoly-in-digital-advertising-1497864602]

Oremus, W., "Who Controls Your Facebook Feed", *Slate*, 03/01/2016 [http://www.slate.com/articles/technology/cover_story/2016/01/how_facebook_s_news_feed_algorithm_works.html]

Osborne, A., "Margaret Thatcher: one policy that led to more than 50 companies being sold or privatised", *The Telegraph*, 08/04/2013 [http://www.telegraph.co.uk/finance/comment/alistair-osborne/9980292/Margaret-Thatcher-one-policy-that-led-to-more-than-50-companies-being-sold-or-privatised.html]

Ostry, J. D., Loungani, P., Furceri, D., "Neoliberalism: Oversold?", *Finance & Development*, Vol. 53, No. 2, June 2016 [https://www.imf.org/external/pubs/ft/fandd/2016/06/ostry.htm]

Owen, T., *Disruptive Power: The Crisis of the State in the Digital Age*, 2015: Oxford

PageFair, *The state of the blocked web 2017: Global Adblock Report*, January 2017 [https://pagefair.com/downloads/2017/01/PageFair-2017-Adblock-Report.pdf]

Palladino, V., "Amazon's Echo Look takes selfies for you, makes clothing suggestions", *ArsTechnica*, 27/04/2017 [https://arstechnica.co.uk/gadgets/2017/04/amazon-echo-look-details-price-uk]

Palmås, K., "Predicting What You'll Do Tomorrow: Panspectric Surveillance and the Contemporary Corporation", *Surveillance & Society*, Vol. 8, No. 3, 2011, pp.338-354

Panagopoulos, C., "All about that base: Changing campaign strategies in U.S. Presidential elections", *Party Politics*, Vol. 22, No. 2, 2015, pp.179-190

Papacharissi, Z., "The virtual sphere: the internet as a public sphere", *New Media & Society*, Vol. 4, No. 1, 2002, pp.9-27

Pasquale, F., *The Black Box Society: The Secret Algorithms That Control Money and Information*, 2015, Harvard Free Press

Pasquale, F., "Two Narratives of Platform Capitalism", *Yale Law & Policy Review*, Vol. 35, No. 1, 2017

Passell, P., "Dr. Jeffrey Sachs, Shock Therapist", *The New York Times*, 27/06/1993 [http://www.nytimes.com/1993/06/27/magazine/dr-jeffrey-sachs-shock-therapist.html]

Pentland, A., "Reality Mining of Mobile Communications: Toward a New Deal on Data", in Dutta, S., and Mia, I., *The Global Information Technology Report 2008-2009: Mobility in a Networked World*, 2009

Penney, J., "Chilling Effects: Online Surveillance and Wikipedia Use", *Berkeley Technology Law Journal*, 2016

Penney, J., "Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study", *Internet Policy Review*, Vol. 6, No. 2, 2017

Perlroth, N. and Sanger, D. E., "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool", *The New York Times*, 12/05/2017 [https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html]

Persily, N., "Can Democracy Survive the Internet?", *Journal of Democracy*, Vol. 28, No. 2, April 2017, pp.65-76

Petersen, S., "Loser Generated Content: From Participation to Exploitation", *First Monday*, Vol. 13, No. 3, 2008

Popper, B., "Google announces over 2 billion monthly active devices on Android", *The Verge*, 17/05/2017 [https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users]

Porter, Z. and Simpson, B., "Preparing to introduce personal health budgets", *Nursing Management*, Vol. 20, No. 6, 2013, pp.18-23

Poster, M., *CyberDemocracy: Internet and the Public Sphere*, 1995, University of California

Powell, J. and Steel, R., "Policy, Governmentality, and Governance", *Journal of Administration and Governance*, Vol. 7, No. 1, 2012

Pressman, A., "Here's How Intel Is Finally Getting Back On Track With Moore's Law", *Fortune*, 05/02/2017 [http://fortune.com/2017/01/05/intel-ces-2017-moore-law]

Privacy International, "Documents obtained by Privacy International show that UK intelligence agencies may analyse our Facebook and Twitter accounts", *Medium*, 17/10/2017 [https://medium.com/@privacyint/documents-obtained-by-privacy-international-show-that-uk-intelligence-agencies-may-analyse-our-c6fcdf2455b7]

Raento, M. and Oulasvirta, A., "Designing for privacy and self-presentation in social awareness", *Personal and Ubiquitous Computing*, Vol. 12, 2008, pp.527-542

Raine, L., and Anderson, J., "Above and Beyond Responses: Part 1", *The Future of Privacy*, Pew Research Center: Internet, Science & Tech, 08/12/2014 [http://www.pewinternet.org/2014/12/18/above-and-beyond-responses-part-1-2]

Ramaswamy, S., "Building a better web for everyone", *Google Blog*, 01/06/2017 [https://www.blog.google/topics/journalism-news/building-better-web-everyone]

Ranchordas, S., "Digital Agoras: Democratic Legitimacy, Online Participation and Uber's Petitions ", *The Theory and Practice of Legislation*, Vol. 5, No. 1, 2017, pp.31-54

Ranzini, G. and Hoek, E., "To you who (I think) are listening: Imaginary audience and impression management on Facebook", *Computers in Human Behaviour*, Vol. 75, 2017, pp.228-235

Rasmussen, T., "Internet and the Political Public Sphere", *Sociology Compass*, Vol. 8, No. 12, 2014, pp.1315-1329

Rheingold, H., *The Virtual Community: Homesteading on the Electronic Frontier*, 1993

Rhodes, R. A. W., *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*, 1997, Open University

Reigeluth, T., "Why data is not enough: Digital traces as control of self and self-control", *Surveillance & Society*, Vol. 12, No. 2, 2014, pp.243-354

Rich, E. and Miah, A., "Mobile, wearable and ingestible health technologies: towards a critical research agenda", *Health Sociology Review*, Vol. 26, No. 1, 2017, pp.84-97

Ritzer, G., "Prosumer Capitalism", *The Sociological Quarterly*, Vol. 56, 2015, pp.413-445

Rose, N. and Miller, P., "Political Power Beyond the State: Problematics of Government", *British Journal of Sociology*, Vol. 43, No. 2, 1992, pp. 172-205

Rose, N., *Powers of Freedom: Reframing Political Thought*, 1999, Cambridge: Cambridge University Press

Rosenberg, J. and Egbert, N., "Online Impression Management: Personality Traits and Concerns for Secondary Goals as Predictors of Self-Presentation Tactics on Facebook", *Journal of Computer-Mediated Communication*, Vol. 17, No. 1, 2011

Rosenberg, "The Business of Google", *Investopedia*, 05/08/2016 [http://www.investopedia.com/articles/investing/020515/business-google.asp]

Royal Swedish Academy of Sciences, *Press Release*, 10/10/2001 [https://www.nobelprize.org/nobel_prizes/economic-sciences/laureates/2001/press.html]

Rouvroy, A. and Berns, T., "Algorithmic Governmentality and Prospects of Emancipation", *Réseaux*, Vol. 1, No. 177, 2013, pp.163-196

Rouvroy, A., "Algorithmic governmentality: a passion for the real and the exhaustion of the virtual", *Transmediale – All Watched Over by Algorithms*, Berlin, 29/01/2015

Rusbridger, A., "The Snowden Leaks and the Public", *The New York Review of Books*, 21/11/2013 [http://www.nybooks.com/articles/2013/11/21/snowden-leaks-and-public]

Rushe, D., "Yahoo $250,000 daily fine over NSA data refusal was set to double 'every week'", *The Guardian*, 12/09/2014 [http://www.theguardian.com/world/2014/sep/11/yahoo-nsa-lawsuit-documents-fine-user-data-refusal]

Rustin-Paschal, N., "Online Behavioral Advertising and Deceptive Campaign Tactics: Policy Issues", *William & Mary Bill of Rights Journal*, Vol. 19, No. 4, 2011, pp.907-926

Sachs, J., *What I did in Russia*, 14/03/2012 [http://jeffsachs.org/2012/03/what-i-did-in-russia]

Savoie, D. J., *Power: Where Is It?*, 2010, McGill-Queen's

Seifert, D., "Samsung's Android browser gets ad blocking capabilities", *The Verge*, 31/01/2016 [https://www.theverge.com/2016/1/31/10880394/samsung-internet-android-ad-content-blocker-adblock-fast]

Seifert, D., "Google restores ad blocker for Samsung browser to the Play Store", *The Verge* 09/02/2016 [https://www.theverge.com/2016/2/9/10949088/google-adblock-fast-restored-play-store]

Schou, J. and Hjelholt, M., "Digitalizing the welfare state: citizenship discourses in Danish digitalization strategies from 2002 to 2015", *Critical Policy Studies*, 2017

Schrage, E., "Hard Questions: Russian Ads Delivered to Congress", *Facebook Newsroom*, 02/10/2017 [https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress]

Schwarz, M., "FACEBOOK FAILED TO PROTECT 30 MILLION USERS FROM HAVING THEIR DATA HARVESTED BY TRUMP CAMPAIGN AFFILIATE", *The Intercept*, 30/03/2017 [https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate]

Schwartz, R. and Halegoua, G. R., "The spatial self: Location-based identity performance on social media", *New Media & Society*, Vol. 17, No. 10, 2015, pp.1643-1660

Scott, J. C., "Everyday Forms of Resistance", *Copenhagen Papers*, No. 4, 1989, pp.33-62

Scott, J. C., *Domination and the Arts of Resistance: Hidden Transcripts*, 1990, New Haven, CT: Yale University Press

Shilton, K., "Participatory Personal Data: An Emerging Research Challenge for the Information Sciences", *Journal of the American Society for Information Science and Technology*, Vol. 63, No. 10, 2012, pp.1905-2915

Shore, C. and Wright, S., *Anthropology of Policy: Perspectives on Governance and Power*, 1997, European Association of Social Anthropologists

Siroker, D., "How Obama Raised $60 Million by Running a Simple Experiment", *Optimizely Blog*, 29/11/2010 [https://blog.optimizely.com/2010/11/29/how-obama-raised-60-million-by-running-a-simple-experiment]

Silcock, R., "What is e-Government?", *Parliamentary Affairs*, Vol. 54, 2001, pp.88-101

Smith, G., "Back doors, black boxes and #IPAct technical capability regulations", *Information Law and Policy Centre*, 10/05/2017 [https://infolawcentre.blogs.sas.ac.uk/2017/05/10/back-doors-black-boxes-and-ipact-technical-capability-regulations]

Smythe, D. W, "On the Audience Commodity and its Work", in Durham, M. and Kellner, D. (Eds.), *Media and Cultural Studies: Keyworks*. 2001, Malden: Blackwell Publishing

Snyder, M., "Self-monitoring of expressive behaviour", *Journal of Personality and Social Psychology*, Vol. 30, 1974, pp.526-537

Solon, O., "You are Facebook's product, not customer", *Wired*, 21/09/2011 [https://www.wired.co.uk/article/doug-rushkoff-hello-etsy]

Solove, D., "Privacy Self-Management and the Consent Dilemma", *Harvard Law Review*, Vol. 126, Issue 7, May 2013, pp.1880-1903

Song, C., Qu, Z., Blumm, N., and Barabási, A., "Limits of predictability in human mobility", *Science*, Vol. 327, 19/02/2010, pp.1018-1021

Sparrow, A., "WhatsApp must be accessible to authorities, says Amber Rudd", *The Guardian*, 26/03/2017 [https://www.theguardian.com/technology/2017/mar/26/intelligence-services-access-whatsapp-amber-rudd-westminster-attack-encrypted-messaging]

Srnicek, N., *Platform Capitalism*, 2016, Polity Press

Stamos, A., "An Update on Information Operations on Facebook", *Facebook*, 06/09/2017 [https://newsroom.fb.com/news/2017/09/information-operations-update]

Statista, *Market share of Android in the United Kingdom (UK) from July 2011 to July 2016*, 2016 [https://www.statista.com/statistics/271240/android-market-share-in-the-united-kingdom-uk]

Stole, D., Hooghe, M., and Micheletti, M., "Politics in the Super-Market: Political Consumerism as a Form of Political Participation", *International Political Science Review*, Vol. 26, No. 3, July 2005, pp.245-269

Storey, G., Reisman, D., Mayer, J., and Narayanan, A., *The Future of Ad Blocking: An Analytical Framework and New Techniques*, 24/05/2017 [https://arxiv.org/abs/1705.08568]

Stoycheff, E., "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring", *Journalism & Mass Communication Quarterly*, Vol. 93, No. 2, 2016, pp.296-311

Stacy, C., "Getting Started Computing at the AI Lab", MIT Artificial Intelligence Laboratory, 07/09/1982 [https://www.academia.edu/1416892/Getting_Started_Computing_at_the_AI_Lab]

Stole, D., Hooghe, M., and Micheletti, M., "Politics in the Super-Market: Political Consumerism as a Form of Political Participation", *International Political Science Review*, Vol. 26, No. 3, July 2005, pp.245-269

Stubbs, P., "Stretching Concepts Too Far? Multi-Level Governance, Policy Transfer and the Politics of Scale in South East Europe", *Southeast European Politics*, Vol. 6, No. 2, November 2005, pp. 66 – 87

Stutzman, F., Capra, R., and Thompson, J., "Factos mediating disclosure in social network sites", *Computers in Human Behaviour*, Vol. 27, 2011, pp.590-598

Su, J., Shukla, A., Goel, S., and Narayanan, A., "De-anonymizing Web Browsing Data with Social Networks", *Proceedings of the 26th International Conference on World Wide Web*, April 2017, pp.1261-1269

Sweeney, L., "Simple Demographics Often Identify People", *Data Privacy Working Paper 3,* Carnegie Mellon University, 2000

Tait, A., "People you may know: is Facebook's friend-finding algorithm putting you at risk?", *New Statesman*, 05/09/2016 [http://www.newstatesman.com/science-tech/security/2016/09/people-you-may-know-facebook-s-friend-finding-algorithm-putting-you]

Tambini, D., Labo, S., Goodman, E., and Moore, M., "The new political campaigning", *Media policy brief 19*, LSE Media Policy Project, 2017

Tang, J., Korolova, A., Bai, X., Wang, X., and Wang, X., "Privacy Loss in Apple's Implementation of Differential Privacy on MacOS 10.12", *Arxiv e-Prints*, 2017 [https://arxiv.org/abs/1709.02753]

Taylor, S. P. J., "Domesday Book and Anglo-Norman Governance", *Transactions of the Royal Historical Society*, Vol. 25, No. 19, 1975, pp.175-193

Teorell, J., Torcal, M., and Montero, J. R., "Political Participation: Mapping the Terrain", in van Deth, J W., Montero, J. R., and Westholm, A. (Eds.), *Citizenship and Involvement in European Democracies: A Comparative Analysis*, 2007, London: Routledge, pp.334-357

Terranova, T., "Free Labor: Producing Culture for the Digital Economy", *Social Text*, Vol. 18, No. 2, Summer 2000, pp.33-58

Thaler, R., and Sunstein, C., *Nudge*, 2008, London: Penguin Books

Thrift, N. J.. "Pass it on: towards a political economy of propensity*", Emotion, Space and Society*, Vol.1, No.2. 2008, pp. 83-96

Toffler, A., *The Third Wave*, 1980, New York: Morrow

Toor, A., "Facebook begins tracking non-users around the internet", *The Verge*, 27/05/2016 [https://www.theverge.com/2016/5/27/11795248/facebook-ad-network-non-users-cookies-plug-ins]

Trotter, J. K., "Public NYC Taxicab Database Lets You See How Celebrities Tip", *Gawker*, 23/10/2014 [http://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546]

Tufekci, Z., "Beware the Smart Campaign", *The New York Times*, 17/11/2012 [http://www.nytimes.com/2012/11/17/opinion/beware-the-big-data-campaign.html]

Tufekci, Z., "Engineering the public: Big data, surveillance, and computational politics", *First Monday*, Vol. 19, No. 7, July 2014 [http://firstmonday.org/ojs/index.php/fm/article/view/4901/4097]

Tufekci, Z., "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency", *Journal on Telecommunications and High Technology Law*, 2015, pp.203-218

Turow, J., *Niche Envy: Marketing Discrimination in the Digital Age*, 2008, MIT Press

Turow, J., *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*, 2012, Connecticut: Yale University Press

Vaidhyanathan, S. and Bulock, C., "Knowledge and Dignity in the Era of 'Big Data'", *The Serials Librarian*, Vol. 66, Nos. 1-4, 2014, pp.49-64

van Brakel, R., and De Hert, P, "Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies", *Journal of Police Studies*, Vol. 20, No. 3, 2011, pp.163-192

van Dijck, J., "'You have one identity': performing the self on Facebook and LinkedIn", *Media, Culture & Society*, Vol. 35, No. 2, 2013, pp.199-215

van Dijck, J., "Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology", *Surveillance & Society*, Vol. 12, No. 2, 2014, pp.197-208

van Schaik, P., Jansen, J., Onibokun, J., Camp, J., and Kusev, P., "Security and privacy in online social networking: Risk perception and precautionary behaviour", *Computers in Human Behaviour*, Vol. 78, 2018, pp.283-297

van Zoonen, L., "From identity to identification: fixating the fragmented self", *Media, Culture & Society*, Vol. 35, No. 1, 2013, pp.44-51

Varian, H, "Computer Mediated Transactions", *American Economic Review*, Vol. 100, May 2010, pp.1-10

Varian, H., "Beyond Big Data", *Business Economics*, Vol. 49, No. 1, 2014, pp.27-31

Verba, S., and Nie, N. H., *Participation in America: Political Democracy and Social Equality*, 1987, Chicago, IL: University of Chicago Press

Villa, D. R., "Postmodernism and the Public Sphere", *American Political Science Review*, Vol. 86, No. 3, Sep 2002, pp.712-721

Vincent, J., "Amazon's Echo look is a minefield of AI and privacy concerns", *The Verge*, 27/04/2017 [https://www.theverge.com/2017/4/27/15447834/amazons-echo-look-ai-analysis-concerns]

Vinthagen, S. and Johansson, A., "'Everyday resistance': exploration of a concept and its theories", *Resistance Studies Magazine*, Vol. 1, 2013

Voigt, P. and von dem Bussche, A., *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 2017, Springer International Publishing, p.113

Wachter, S., Mittelstadt, B., and Floridi, L., "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law*, Vol. 7, No. 2, 2017, pp.76-99

Weber, M., *Economy and Society: an Outline of Interpretative Sociology*, 1978, Berkeley

Weber, S., *The Internet: Transforming Power of Technology*, 2003, Chelsea House Publishers

Whittaker, J., "Why I Left Google", *Medium*, 05/04/2015 [https://medium.com/@docjamesw/why-i-left-google-c170e6165f2a]

Wiegand, T., "There is Only One Presumption of Innocence", *Netherlands Journal of Legal Philosophy*, Vol. 42, 2013, p.196

Wilkinson, R., and Pickett, K., "Margaret Thatcher made Britain a less, not more, desirable place to do business", *The Guardian*, 10/04/2013 [http://www.theguardian.com/commentisfree/2013/apr/10/inequality-margaret-thatcher-britain-desirable-business]

Williams, C. B. and Gulati, G., J., "Digital Advertising Expenditures in the 2016 Presidential Election", *Social Science Computer Review*, 2017, pp.1-16

Williams, R. W., "Politics and Self in the Age of Digital Re(pro)ducibility", *Fast Capitalism*, Vol. 1, No. 1, 2005

Williamson, J., "What Washington Means by Policy Reform", in Williamson, J. (Ed.), *Latin American Adjustment: How Much Has Happened?*, 1990

Williamson, J., *Did the Washington Consensus Fail?*, 2002

Woodward, B., *Veil: The Secret Wars of the CIA 1981-1987*, 1987: New York

World Wide Web Foundation, *History of the Web* [https://webfoundation.org/about/vision/history-of-the-web]

Yeung, K., "'Hypernudge': Big Data as a mode of regulation by design", *Information, Communication & Society*, Vol. 20, No. 1, 2017a, pp.118-136

Yeung, K., "Algorithmic Regulation: A Critical Interrogation", *Regulation & Governance*, 2017b

Yildiz, M., "E-government research: Reviewing the literature, limitations, and ways forward", *Government Information Quarterly*, Vol. 24, No. 3, March 2007, pp. 646-665

Zittrain, J., "Engineering an Election", *Harvard Law Review Forum*, No. 127, 2014

Zlatolas, L. N., Welzer, T., Heričko, M., Hölbl, M., "Privacy antecedents for SNS self-disclosure: The case of Facebook", *Computers in Human Behaviour*, Vol. 45, 2015, pp.158-167

Zuboff, S., *The Psychological and Organizational Implications of Computer-Mediated Work*, 1981: Center for Information Systems Research, MIT

Zuboff, S., *In The Age Of The Smart Machine: The Future of Work and Power*, 1988, New York

Zuboff, S., "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information and Technology*, Vol. 30, 2015, pp.75-89

Zuboff, S., "The Secrets of Surveillance Capitalism", *Frankfurter Allgemeine Zeitung*, 05/03/2016 [http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html]

Zuckerman, E., *Me and my metadata – thoughts on online surveillance*, 03/07/2013 [http://www.ethanzuckerman.com/blog/2013/07/03/me-and-my-metadata-thoughts-on-online-surveillance]

Zwick, D., "DEFENDING THE RIGHT LINES OF DIVISION: Ritzer's Prosumer Capitalism in the Age of Commercial Customer Surveillance and Big Data", *The Sociological Quarterly*, Vol. 56, 2015, pp.484-498